CONCEPTUALIZATIONS OF CONSTITUTIONAL PRIVACY AND THEIR IMPLICATIONS IN FEDERALDATA VEILLANCE

Martin Kuhn

A dissertation submitted to the faculty of the University of North Carolina at Chapel Hill in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the School of Journalism and Mass Communication.

Chapel Hill
2006

Approved by
Advisor: Cathy Packer, Ph.D.
Reader: Ruth Walden, Ph.D.
Reader: Anne Klinefelter, J.D.
Reader: Paul Jones, M.F.A.
Reader: Frank Fee, Ph.D.

© 2006
Martin Kuhn
ALL RIGHTS RESERVED

ABSTRACT

MARTIN KUHN: Conceptualizations of Constitutional Privacy and Their Implications in Federal Dataveillance
(Under the direction of Cathy Packer, Ph.D.)

The federal government's use of new data technologies, specifically knowledge discovery in databases (KDD) applications, in counterterrorism efforts presents a serious challenge to existing constitutional privacy protections. The purpose of this dissertation is to explore whether this use of KDD technology infringes upon a constitutional right to information privacy. A broad discussion of how the constitutional right to privacy in general and information privacy in particular has been conceptualized by the courts is presented. Following a review of privacy scholarship, traditional legal case analysis is used to identify privacy conceptualizations in three types of privacy cases: U.S. Supreme Court First Amendment anonymous speech and association cases, Fourth Amendment privacy cases, and those Supreme Court and U.S. Circuit Courts of Appeal cases involving information privacy claims.

Five conceptualizations of privacy are discussed. Three were found in the privacy scholarship: privacy as space, privacy as secrecy, and privacy as information control. The analysis of U.S. Supreme Court and U.S. Circuit Courts of Appeal information privacy cases reveals a newly emerging conceptualization of privacy, privacy as confidentiality. Under this conceptualization, individuals are empowered to compel government to safeguard the personal information it has forced them to surrender and to hold state actors responsible for

knowing which constitutional information privacy interests are clearly established. This is a significant departure from the first three conceptualizations because the responsibility for protecting personal information resides with the government rather than the individuals to whom the information belongs.

The most significant finding presented in this dissertation is that none of these four conceptualizations are sufficient to protect privacy against KDD dataveillance. Since these applications create new knowledge rather than access and manipulate existing information, a new conceptualization, privacy as knowledge control, is needed. Should the courts adopt and vigorously apply a privacy-as-knowledge-control conceptualization of privacy, individuals will have the right to be informed that new information regarding them has been created, that the government has information safeguards in place to protect this new knowledge, and that they have the right to challenge the government on constitutional grounds regarding the use of the discovered knowledge.

For Rebecca Michelle

ACKNOWLEDGMENTS

I would like to express my gratitude to the many individuals who made this dissertation possible. I am particularly indebted to my dissertation committee chair, Cathy Packer, Ph.D., who welcomed me as an advisee upon the death of my original advisor. She encouraged my legal exploration of new technologies, spent many hours guiding me through the dissertation process, and forgot that she was entitled to weekends, vacations, and holidays. The members of my dissertation committee also have my sincerest thanks. Throughout the entire process, Ruth Walden, Ph.D., Frank Fee Ph.D., Paul Jones, M.F.A., and Anne Klinefelter, J.D., each dedicated their time and expertise to the project and provided me with endless encouragement. The knowledge and friendship they shared made this project bothfruitful and enjoyable.

I would also like to thank my wife, Rebecca Kuhn, not only for her encouragement during the dissertation process, but for her belief in my abilities as a scholar and teacher throughout my doctoral program. Without her constant love and support through the coursework, conferences, committees, and comprehensive examinations, this dissertation could never be. I am also grateful to my parents, Martin and Evelyn Kuhn, for instilling in me at a young age an appreciation for books, learning, and education. My passion for intellectual exploration derives directly from the example they set so long ago. To my many family members, friends, and colleagues who listened to my endless chatter about information privacy and dataveillance, thank you. Lastly, I would like to thank Dr. Margaret "Peggy" Blanchard for bringing me to Chapel Hill.

TABLE OF CONTENTS

CHAPTER I

INFORMATION PRIVACY AND GOVERNMENT DATAVEILLANCE[1]

In the opening decades of the Information Age[2] two developments have renewed a scholarly and public interest in the constitutional right to information privacy. First, new and cost-efficient information technologies have enabled the processing of massive quantities of data about millions of individuals. This has allowed large database companies (data aggregators)[3] to build digital dossiers[4] on individual consumers.

---

[1] Roger A. Clarke, *Information Technology and Dataveillance*, COMM. OF THE ACM, May 1988, at 499. Clarke is a consultant specializing in strategic and policy aspects of *e*Business, information infrastructure, and data surveillance and privacy, and he has been in the information technology industry for thirty-five years. He defined dataveillance as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" and further differentiated between personal surveillance (surveillance of a specific individual for a particular purpose) and mass surveillance (surveillance of a group in order to identify specific individuals for further investigation).

[2] Glossary, A Guide for Developing Countries, http://cyber.law.harvard.edu/readinessguide/glossary.html (last visited Sept. 26, 2005) (defining Information Age as the current stage in societal development that began to emerge at the end of the twentieth century and is marked by the increased production, transmission, consumption of, and reliance on information).

[3] Companies like ChoicePoint, Experian, Acxiom, and LexisNexis began purchasing databases from hundreds of private-sector companies, institutions, and organizations. The data were combined into larger and larger databases. Aggregators "packaged" personal information and either sold data directly or contracted for access to the digital dossiers in their massive data warehouses. *See* ROBERT O'HARROW, JR., NO PLACE TO HIDE 1-6 (2005).

[4] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 2 (2004). Solove is an associate professor at the George Washington University Law School and has authored a number of books and law review articles about information privacy and new database technologies. He wrote, "[D]ossiers are being constructed about all of us. Data is digitized into binary numerical form, which enables computers to be able to store and manipulate it with unprecedented efficiency. There are hundreds of companies that are constructing gigantic databases of psychological profiles, amassing data about an individual's race, gender, income, hobbies, and purchases. Shards of data from our daily existence are now being assembled and analyzed—to investigate backgrounds, check credit, market products, and make a wide variety of decisions affecting our lives."

Second, federal intelligence and law enforcement agencies responded to the terrorist attacks of September 11, 2001, by using the new information technologies to access privately held data in an effort to prevent additional attacks.

Once the technology needed for building digital dossiers emerged, related technologies capable of "mining" these records for predictive patterns were developed.[5] Since 2001 the United States Intelligence Community (USIC)[6] has considered data aggregation and analysis technology to be a primary weapon in counterterrorism. John Poindexter, former director of DARPA's[7] Information Awareness Office, explained, "The only way to detect these terrorists is to look for patterns of activities that are based on observations from past terrorist attacks as well as estimates about how terrorists will adapt to our measures to avoid detection."[8] Data mining, more accurately known as

---

[5] Dr. Tony Tether, Director, Defense Advanced Research Projects Administration, Written Statement Submitted to the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census of the House Committee on Government Reform 1 (May 6, 2003), http://reform.house.gov/UploadedFiles/DARPA%20testimony.pdf (defining data mining as the use of clever statistical techniques to comb through large amounts of data to discover previously unknown, but useful patterns for building predictive models and as finding statistical correlations to discover unknown behavior patterns, which are then used to build a predictive model); *see also* DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES, GAO-04-548, at 1 (2004) [hereinafter FEDERAL EFFORTS] (defining data mining as the application of database technology and techniques—such as statistical analysis and modeling—to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results); *see also* Tal Z. Zarsky, *"Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE SYMP. L. & TECH. 1 (2002/2003) (Quoting Usama Fayyad, father of data mining technologies, in U.M. FAYYAD ET. AL., FROM DATA MINING TO KNOWLEDGE DISCOVERY: AN OVERVIEW, IN ADVANCES IN KNOWLEDGE DISCOVERY AND DATA MINING (1996) wherein Fayyad defined data mining as the "nontrivial process of identifying valid, novel, potentially useful and ultimately understandable patterns in the data").

[6] The term "United States Intelligence Community" or USIC refers to the group of federal agencies and departments charged with gathering intelligence, both foreign and domestic, in an effort to protect the nation from future terrorist attacks or other external threats. Examples include the Central Intelligence Agency (CIA), the Department of Defense (DOD), and the Department of Homeland Security (DHS).

[7] The Defense Advanced Research Projects Administration.

[8] John M. Poindexter, *Security with Privacy* 3 (adapted from *Finding the Face of Terror in Data*, N.Y. TIMES, Sept. 10, 2003, at A25), http://www.maxwell.syr.edu/campbell/library%20Papers/event%20papers/ISHS/Poindexter.pdf. Poindexter also noted that "terrorists operate worldwide, and information about their activities is mixed in with data

knowledge discovery in databases (KDD),[9] is the technology capable of distinguishing these patterns within millions of dossiers and identifying those subjects matching the predefined patterns of possible terrorists.

This type of electronic surveillance of personal data (dataveillance) invokes substantial privacy concerns under the First and Fourth amendments and the fledgling constitutional right of informational privacy, and the fact that a constitutional right of information privacy has not yet been clearly defined complicates matters. Dataveillance using KDD raises First Amendment concerns that individuals may self-censor for fear that data regarding their expressive activities and personal associations might match a federal counterterrorism data pattern. These counterterrorism practices also raise Fourth Amendment concerns that dataveillance is a search without probable cause and violates an individual's reasonable expectation of privacy regarding his or her personal information. Lastly, the Supreme Court has recognized but not yet defined a constitutional right of information privacy – a right for individuals to avoid the "disclosure of personal matters"[10]-- in the penumbras and emanations of the Bill of Rights.

---

about innocent people;" *see also* Paul Rosenzweig, *Civil Liberty and the Response to Terrorism*, 42 DUQ. L. REV. 663, 679 (2004). "Virtually every terrorism expert in and out of government believes there is a significant risk of another attack. Unlike during the Cold War, the threat of such an attack is asymmetric. . . . [T]he Soviets created 'things' that could be observed, the terrorists create only transactions that can be sifted from the noise of everyday activity only with great difficulty."

[9] David Jensen, Data Mining in Networks (Dec. 11, 2002), http://kdl.cs.umass.edu/people/jensen/papers/nrcdbsse02/slide10.html. According to Professor Jensen, the term "knowledge discovery" is preferable to "data mining" because "these technologies do not 'mine for data' they 'mine for knowledge'—they look through data to find knowledge;" *see also* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1456 (2001). "Information is not the key to power in the Information Age—knowledge is. Information consists of raw facts. Knowledge is information that has been sifted, sorted, and analyzed."

[10] Whalen v. Roe, 429 U.S. 589, 598-600 (1977).

The purpose of this dissertation is to explore whether the U.S. government's use of KDD technologies infringes upon a constitutional right to information privacy. It explores what the courts have said about the right to privacy in general and information privacy in particular in First Amendment anonymous speech and association cases, in Fourth Amendment privacy cases, and information privacy cases in the U.S. Circuit Courts of Appeal. Conceptualizations of privacy and information privacy that emerge in the case analysis are then applied to the government's use of KDD dataveillance in order to evaluate its constitutionality. This research is presented in the context of a broad discussion of what constitutes information privacy and whether information privacy needs to be defined differently in order to protect both individual privacy and national security.

This is an important research topic primarily because, as Daniel J. Solove wrote, "[T]he existing law protecting information privacy has not adequately responded to the emergence of digital dossiers."[11] Database technologies have emerged quickly, and as technology policy expert Charles Weiss noted: "American values on privacy were defined in a previous, less technological era. These values need to be reexamined and redefined for a modern era of data mining and knowledge discovery."[12]

Any successful solution may need to be built upon a new conceptualization of the constitutional right to information privacy. As Weiss argued, "[T]he legal responses to advances in technology have so weakened the limits on the government's ability to gather

[11] Solove, *supra* note 4, at 9.

[12] Charles Weiss, *The Coming of Knowledge Discovery: A Final Blow to Privacy Protection?*, 2004 U. ILL. J.L. TECH. & POL'Y 253, 271 (2004). Weiss holds the Chair of Science, Technology, and International Affairs at the Edmund A. Walsh School of Foreign Service at Georgetown University and was the first science and technology advisor to the World Bank.

aggregate information that a systematic review of the safeguards to privacy is now necessary, even if this requires a reexamination of well-settled constitutional precedent."[13] This dissertation provides such a reexamination.

Digital Dossiers and KDD

Today's data technologies have roots in the realms of both consumer marketing and federal bureaucracy. In the 1950s and 1960s many private companies began collecting data in order to better identify who was purchasing their products or services.[14] Initially, they used data grouping[15] and matching[16] to better target their products and advertising. For instance, an automobile company could separate women who purchased a particular model car in Chicago within a specific time period from other people in its database.

Data matching is used to build more detailed consumer records for a specific market segment. For example, a woman's name might appear in a database containing the group "women who purchased Buicks in Chicago last month" and also in one containing women who purchased a baby crib within the last year. A computer could

[13] *Id*. at 270.

[14] Over time demographic, geographic, and eventually psychographic information was gathered and used to better "target" both product development and advertisements to prospective customers.

[15] The term "grouping" refers to sorting records in a database by a particular variable or set of variables such as age, gender, or consumer behavior.

[16] Clarke, *supra* note 1, at 504. He defined computer matching as "the exploration of data maintained by two or more personal-data systems, in order to merge previously separate data about large numbers of individuals; *see also* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEBSITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 324 (2000) (noting that marketers began to define targeted "clusters" such as "Pools & Patios (affluent Caucasian empty-nest couples), Soccer & Braces (families with elementary school youngsters), Blue Blood Estates (very wealthy), Shot Guns & Pick-ups (rural good ole boys), Black Enterprise (upwardly mobile African-Americans), even Grumpies (grim, ruthless, upwardly mobile professionals—who use lots of credit cards and use them frequently)").

match her records in each database and create a new record containing the information from both sources. She might then be grouped into a new data set called "New Driving Mothers," a valuable list for companies producing baby car-seats. Americans have grown accustomed to corporations collecting their personal data, and they seem to value having marketing messages and products tailored specifically to their tastes.[17]

The government also used computers to process and store data. Privacy historian Robert Ellis Smith wrote, "By the 1960s . . . America had become a credentialed society, demanding personal qualifications to receive the coveted benefits of education, employment, health care, licenses, and social services."[18] The vast amount of "qualifying" information began to overwhelm many departments and agencies at the local, state, and federal levels. A national data center was proposed in the mid-1960s to provide "more coherent data management to support economic and sociological research," [19] but public sentiment was strongly unfavorable and the proposal was eventually dropped.[20]

---

[17] *See* Markle Foundation, Creating a Trusted Information Network for Homeland Security: Second Report of the Markle Foundation Task Force 30 (Dec. 2003) [hereinafter Markle Report II], *available at* http://www.markletaskforce.org/.

[18] SMITH, *supra* note 16, at 314-15.

[19] Clarke, *supra* note 1, at 500; *see also* United States Department of Health, Education & Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Community on Automated Personal Data Systems* 9-10 (1973) (explaining the government's need for storing and analyzing personal data as such: "[A]dministrative data are needed for everyday management of transactions. Statistical data are needed for making judgments about people's character and qualification; e.g., in making suitability determinations for employment, commercial credit, welfare assistance, tuition-loan aid, or disaster relief, and warning that: "The demand generated by all these uses for personal data, and for record-keeping systems to store and process them, challenges conventional legal and social controls on organizational record keeping. Records about people are becoming both more ubiquitous and more important in everyday life.").

[20] *See, e.g.,* ALAN WESTIN, PRIVACY AND FREEDOM 317-20 (1967) (providing an overview of the press reaction to the national data center, the Congressional hearings that resulted, and the eventual tabling of the proposal); *see also* K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data,* 5 COLUM. SCI. & TECH. L. REV. 2 (2004), http://www.stlr.org/cite.cgi?volume=5&article=2

Since the development of a national data center seemed politically unpopular, the federal government has never openly developed a central data storage and processing facility. Data technologies therefore primarily emerged from the private sector.[21] Meanwhile, government agencies and departments at the local, state, and federal levels continued to collect, store, and utilize data independently of one another.

Eventually mass marketers began to develop strategies for targeting individual consumers rather than broad market segments, and publicly held data was central to this purpose. Companies began purchasing public records containing identifiable information from federal, state, and local governments.[22] This allowed data aggregators to add millions of names, addresses, and social security numbers to their largely anonymous marketing data. The public records also infused consumer dossiers with data such as tax payments, auto registrations, arrest records, veteran status, political party affiliations,

---

(arguing that after the elimination of funding for the Terrorist Information Awareness (TIA) project in 2003, large database projects and new technologies should never be cancelled because the technologies will be developed anyway by the private sector and without public oversight. If projects like the proposed national data center and TIA were allowed to progress, public discourse would assure that privacy protections would be built into the technical and operational architecture.).

[21] *See* SIMSON GARFINKLE, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 35 (2001). Garfinkle argued that "we blew it" by not completing the national data center. He thought it would have headed off the future excesses of the credit reporting industry and could have prevented the sea of errors that exist in the plethora of private databanks today. Moreover, with a public system, uses of the data for purposes other than those originally intended would have been debated in public, rather than proposed and approved behind closed doors; *see also* Taipale, *supra* note 20, at ¶6 (arguing that "*not* proceeding with government funded research and development of these technologies (in which political oversight can incorporate privacy protecting features into the design of the technologies) will ultimately lead to a diminution in privacy protection as alternative technologies developed without oversight (either through classified government programs or proprietary commercial development) are employed in the future, since those technologies may lack the technical features required to support legal and procedural mechanisms to protect privacy and civil liberties).

[22] CHARLES J. SYKES, THE END OF PRIVACY 29 (1999) (noting, "Governments are making tens of millions of dollars selling public records to junk mailers and other businesses" and that efforts to limit access to publicly held personal information "have been halfhearted, at best"); *see also* ERIK LARSON, THE NAKED CONSUMER: HOW OUR PRIVATE LIVES BECOME PUBLIC COMMODITIES 239 (1992) (asserting that the government's practice of selling compelled, personal information to marketers was eroding public trust in government and thus "any new [privacy] law must give individuals real, effective control over how the information they give to government is used").

vital statistics (height, weight, and eye color), property ownership data, census data, and marital status.[23] This resulted in a new market for highly detailed digital dossiers. One commentator noted that digital dossiers were becoming "commodities, bought and sold like bags of potato chips and six packs of beer."[24]

Digital dossiers also contain data collected as people move through society doing small things such as purchasing products with credit cards, filling out consumer surveys, or voting. Most individuals do not realize that they are leaving behind a data trail that amounts to a psychographic self-portrait. Julie E. Cohen, a Georgetown University law professor, opined that the "picture" created by an individual's "record-generating behaviors" is in some respects more "detailed and intimate than that produced by visual observation."[25] Simson Garfinkle, research fellow at the Center for Research on Computation and Society at Harvard University, referred to his transactional data trail as his "data shadow."[26] The composite resulting from the collection of the data has also been referred to as one's "digital biography,"[27] one's "information plus,"[28] and one's

---

[23] Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1194-95 (2002). "Public records . . . are often a principle source of information for the private sector in the construction of their databases. Marketers stock their databases with public record information, and the uses to which these databases are put are manifold and potentially limitless."

[24] Andrew J. McClurg*, A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 142 (2003).

[25] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425-26 (2000); *see also* Stan Karas, *Privacy, Identity, Databases,* 52 AM. U. L. REV. 393, 439 (2002) (explaining that "consumption patterns . . . as revealed by consumer records" allow third parties to "pinpoint not only the person's socioeconomic status, but also his or her cultural and social inclinations.").

[26] GARFINKLE, *supra* note 21, at 70. He wrote: "[M]y data shadow is largely beyond my control. Scattered across the computers of a hundred different companies, my shadow stands at attention, shoulder-to-shoulder with an army of other data shadows inside the databanks of corporations and governments all over the world."

[27] Solove, *supra* note 23, at 1141. "Consolidating various bits of information, each in itself relatively unrevealing, can, in the aggregate, begin to paint a portrait of a person's life. I refer to this as a 'digital biography'."

"data self."[29] In this dissertation the term "digital dossier" is used to refer to an individual's compiled, digital record. Eventually, KDD technologies developed allowing analysts to predict the future behavior of consumers based on data patterns found in their dossiers.[30]

The new security challenges brought by 9-11 have encouraged traditional law enforcement and intelligence agencies to rely on access to data held by the private sector and on KDD processes. This is exemplified by the ad hoc public-private data partnerships that emerged immediately after 9-11. For instance, a travel Website used by the 9-11 hijackers revealed to the FBI "the patterns the hijackers followed and identified others who fit a similar profile,"[31] and an airline, JetBlue,® turned over the names and addresses of five million passengers for use in a military data mining study on risk assessment.[32] The previous "outflow" of information from public databases to private-sector data companies has reversed direction. There are currently no restraints on government access to commercial data accessed through voluntary disclosure resulting from a government

---

[28] Karas, *supra* note 25, at 424 (explaining that privacy law and scholarship seek to protect not mere information relating to a person, but rather "information plus," information that is expressive of one's self).

[29] McClurg, *supra* note 24, at 142.

[30] Lee Tien, Symposium Article, *Privacy, Technology and Data Mining*, 30 OHIO N.U. L. REV. 389, 395 (2004) (explaining the difference between mere data matching and KDD as the difference between looking up material that is "in" a database and using data mining to discover patterns and relationships in the data that "we humans might not think of on our own").

[31] Robert S. Mueller, III, Director, FBI, Partnership and Prevention: The FBI's Role in Homeland Security, Commonwealth Club of California ¶17 (April 19, 2002), http://www.fbi.gov/pressrel/speeches/speech041902.htm.

[32] Markle Report II, *supra* note 17, at 10-11; *see also* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1096 (2002) (describing the resulting information flow "when the government requests private sector records for particular investigations or compels their disclosure by subpoena or court order").

request.[33] According to James Dempsey and Laura Flint, executive director and staff counsel at the Center for Democracy and Technology, "Third parties that hold consumer information often comply with such requests because they want to be helpful to the government or because compliance seems to be the path of least resistance."[34]

Along with access to private databases, federal law enforcement and intelligence agencies have come to rely on KDD technology.[35] A Markle Foundation[36] task force on national security and information technology reported that private data and KDD technology "might be used not only for investigations of specific people (for example, to help find associates of a suspected terrorist) but also to perform large-scale data analysis and pattern discovery in order to discern potential terrorist activity by unknown individuals."[37] Agencies began designing and implementing in-house data mining projects and also contracting with companies like ChoicePoint and Acxiom for national

---

[33] A proposed partnership between the United States Intelligence Community (USIC) and private-sector data companies was written into the 2005 National Intelligence Strategy: "The Program Manager, Information Sharing Environment, in conjunction with the Chief Information Officer, will develop a plan to facilitate the means for sharing terrorist information among all appropriate federal, state, local, and tribal entities, and the *private sector* (emphasis added);" *see* Staff of the Office of the Director of National Intelligence, The National Intelligence Strategy of the United States of America: Transformation though Integration and Innovation 11 (Oct. 26, 2005) [hereinafter National Intelligence Strategy], http://www.dni.gov/NISOctober2005.pdf.

[34] James X. Dempsey & Laura M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1476 (2004).

[35] FEDERAL EFFORTS, *supra* note 5, at 2. Between May 2003 and April 2004, the GAO audited 128 federal departments and agencies in an attempt to identify ongoing or planned data mining efforts and found that 52 departments were conducting 131 data mining programs.

[36] The John and Mary R. Markle Foundation, Inc. was founded to "promote the advancement and diffusion of knowledge" and the "general good of mankind." Since 1988 the foundation has focused on three main program areas: Policy for a Networked Society, Healthcare, and Interactive Media for Children. Recently, the foundation has identified the "modernization of the complex and over-burdened healthcare system and the strengthening of our nation's security against the threat of terrorism" as the two "most critical issues of our time." Additional information about the foundation is available at http://www.markle.org/index.php.

[37] Markle Report II, *supra* note 17, at 31. One key concern is mission creep wherein information collected for counterterrorism purposes by the government will at some point in the future be used for another, secondary, purpose.

security, database solutions.[38] The new security posture was described as follows in the first Markle task force report on information technology and national security: "Information and information processing is to homeland security as the brain is to the human body."[39]

A key privacy concern is that the use of KDD technology in counterterrorism efforts amounts to government surveillance of individuals not suspected of any crime. Even before the terror attacks of 9-11 some scholars warned of a government, tempted by new data technologies, that was ready to plunge American citizens into an Orwellian existence.[40] In 1999 Charles Sykes opined, "By invoking fears of drug cartels, kidnappings, and international terrorism, the FBI has sought the power to be a fly on the wall in the new information age."[41] Some commentators now have gone as far as to compare the Bush Administration's response to the terror attacks of 9-11 to the repressive domestic surveillance policies of J. Edgar Hoover[42] and the USIC's use of KDD to the

[38] *Id.* at 30. Governments can readily buy data sets from data aggregators, who can deliver the data to government users in any format necessary for immediate analysis; *see generally* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C.J. INT'L L. & COM. REG. 595, 597-99 (2004) (relating how the Electronic Privacy Information Center (EPIC) sought information pertaining to ChoicePoint, LexisNexis, Experian, Dun & Bradstreet, and Database Technologies Online and received over 1,500 government documents pertaining to companies that sell personal information to the government, which led to the revelation that "the database companies are extremely solicitous to government and actually design the databases for law enforcement use").

[39] Markle Foundation Task Force, Protecting America's Freedom in the Information Age 38 (Oct. 2002) [herinafter Markle Report I], http://www.markletaskforce.org/.

[40] *See e.g.* O'HARROW, JR., *supra* note 3; and DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998).

[41] SYKES, *supra* note 22, at 156.

[42] John D. Podesta & Raj Goyle, *Lost in Cyberspace? Finding American Liberties in a Dangerous Digital World*, 23 YALE L. & POL'Y REV. 509, 510-16 (2005).

"general warrants" issued by the English kings in the seventeenth and eighteenth centuries.[43]

The government has recognized the privacy threat posed by its domestic dataveillance. The 9-11 Commission Report [44] acknowledged the possibility that increased federal surveillance powers might lead to civil rights violations: "This shift of power and authority to the government calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life."[45] More recently, the 2005 National Intelligence Strategy referred to the maintenance of such a balance as an enterprise objective and noted, "[W]e must . . . perform our duties under law in a manner that respects the civil liberties and privacy of all Americans."[46] The nature of that which the government has a constitutional duty to protect remains a subject of some debate.

---

[43] "In some ways, mass dataveillance looks very much like the general warrants that the framers of the Fourth Amendment to the Constitution were determined to prohibit. . . . Mass dataveillance, like general warrants, allows the government to scan a great deal of innocent information in the course of fishing for signs of guilt. And in the process, it threatens both privacy and equality, and diverts government resources away from more effective responses to terrorism." JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE 23 (2004); *see infra* p. 13 and note 47.

[44] The Congressional commission of five Democrats and five Republicans (established by the 2002 Intelligence Authorization Act for FY2003, Pub. L. No.107-306, Title VI §§ 601-611, 116 Stat. 2383 (2002)) was charged with making recommendations intended to ready America for stopping future terrorist attacks.

[45] FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 394 (Authorized 1st Ed., 2004). The commission made three recommendations to safeguard civil liberties: [1] The President should safeguard the privacy of individuals when determining guidelines for information sharing among government agencies and between government agencies and the private sector; [2] The burden of demonstrating that controversial provisions of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act of 2001), materially enhance security and that they are subject to adequate oversight when they come up for renewal; and [3] An executive branch board should be established to oversee adherence to the guidelines the 9/11 commission recommends in the interest of protecting civil liberties.

[46] National Intelligence Strategy, *supra* note 33.

The word privacy does not appear in the U.S. Constitution. However, today's privacy protections can be traced back to the ratification of the Bill of Rights, through which the Founders sought to protect individual rights including private property rights from the fledgling central government. The Fourth Amendment in particular protected citizens from the general warrants that were common under English rule.[47] Prior to the late nineteenth century, no jurist or legal scholar made the argument that personal privacy warranted constitutional protection.

While the constitutional right of privacy exists separately from the common law privacy torts, conceptualizations of what constitutes the constitutional right of privacy clearly trace their roots to the common law. Seventy-five years before the U.S. Supreme Court explicitly recognized a constitutional right of personal privacy, Samuel D. Warren and Louis D. Brandeis provided the foundation for a common law right of personal privacy in their seminal 1890 *Harvard Law Review* article, "The Right to Privacy."[48] They argued that individuals had a right "to be let alone"[49] and that common law remedies under the general legal rules regarding slander and libel and the "law of literary and artistic property" could be used to enforce this right to privacy. During the next

[47] BLACK'S LAW DICTIONARY 1616 (8th ed. 2004). A general warrant is defined as [1] "a warrant issued by the English Secretary of State for the arrest of the author, printer, or publisher of a seditious libel, without naming the person to be arrested" and [2] "a warrant that gives a law-enforcement officer broad authority to search and seize unspecified places or persons; a search or arrest warrant that lacks a sufficiently particularized description of the person or thing to be seized or the place to be searched."

[48] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[49] *Id*. at 195. Their article argued that common law should provide remedy for invasions of privacy, and they cite Judge Thomas Cooley as the source of the phrase "right to be let alone;" *see* THOMAS MCINTYRE COOLEY ON TORTS, 2d ed., p. 29 (Callagan 1888). "The right to one's person may be said to be a right of complete immunity: to be let alone."

seven decades states adopted privacy statutes,[50] and state courts recognized privacy torts[51] that were based upon the Warren and Brandeis article.

Thirty-eight years after he first asserted that a right to privacy existed in the common law, Justice Louis Brandeis argued that there also was a constitutional basis for a right to privacy under the Fourth Amendment. In his dissent in *Olmstead v. United States*, Brandeis wrote: "The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. . . . They conferred, as against the government, the right to be let alone -- the most comprehensive of rights and the right most valued by civilized men."[52] *Olmstead* involved wiretapping, and the majority ruled there was no invasion of privacy because there was no physical incursion into the home in question. Brandeis refuted this purely "physical" conceptualization of privacy and wrote that the Fourth Amendment guaranteed protection for Americans "in their beliefs, their thoughts, their emotions and their sensations" as well as in their property.[53]

---

[50] *See* Electronic Privacy Information Center, Privacy Laws by State, http://www.epic.org/privacy/consumer/states.html (providing a completed and updated list of state privacy statutes); *see also* Privacilla.org, Special Report, How U.S. State Law Quietly Leads the Way in Privacy Protections 18-24 (July 2002), http://www.privacilla.org/releases/Torts_Report.pdf (providing a state-by-state listing of key cases, statutes, and sources).

[51] *See generally* William J. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960) (recognizing the following four privacy torts: [1] Intrusion upon Seclusion (RESTATEMENT (SECOND) OF TORTS § 652B (1977), This tort allows plaintiffs to seek remedy for the invasion of their "solitude or seclusion" or "private affairs or concerns" if the intrusion is "highly offensive to a reasonable person."); [2] False Light (RESTATEMENT (SECOND) OF TORTS § 652E (1977), This tort allows plaintiffs to seek remedy when they are portrayed in a false light that "is highly offensive to a reasonable person" because the defendant publicly disclosed certain matters or information.); [3] Public Disclosure of Private Facts (RESTATEMENT (SECOND) OF TORTS § 652D (1977)), This tort allows plaintiffs to seek remedy for the disclosure of a private fact that is "highly offensive to a reasonable person" and not about a matter of public concern.); and [4] Appropriation (RESTATEMENT (SECOND) OF TORTS § 652C (1977), This tort allows plaintiffs to seek remedy when their "name or likeness" is appropriated for the defendant's "use or benefit.").

[52] 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[53] *Id.*

It wasn't until 1965 in *Griswold v. Connecticut*[54] that the Supreme Court recognized that a constitutional right to personal privacy was implied in the "penumbras" and "emanations" of the protections guaranteed in the Bill of Rights. For the majority, Justice William O. Douglas wrote:

> [S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment.[55]

Because privacy has only been recognized as a constitutional right for forty years, it is no surprise that it is still vaguely defined. This makes conceptualizing a constitutional right of information privacy, typically conceived of as a subset of this more general privacy right, more difficult.

Not until 1977, in *Whalen v. Roe*,[56] did the Supreme Court finally recognize a constitutional right to information privacy. In *Whalen* the U.S. Supreme Court upheld a New York state statute that required doctors to submit to the New York Department of Health forms containing the personal information of patients for whom the doctors had prescribed potentially addictive medications. Justice John Paul Stevens wrote for the

[54] 318 U.S. 479 (1965). The Court struck down a Connecticut law making it illegal for married couples to purchase contraceptives because it was an unconstitutional invasion of couple's fundamental liberty to define their most intimate relationships.

[55] *Id*. at 484.

[56] 429 U.S. 589 (1977).

Court that the statute in question did not, on its face, invade "a constitutionally protected zone of privacy."[57] Nevertheless, the landmark opinion distinguished between two different privacy interests: "One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[58] Information privacy was thus distinguished from decisional privacy.

In *Whalen* the Court said that information privacy was a "liberty" protected by the Fourteenth Amendment from abridgement by the states. There was no other explanation in the text of the opinion as to the source of the constitutional protection for information privacy. The only explanation was in a footnote citing several privacy cases, noting Brandeis's characterization of privacy as "the right to be let alone,"[59] and quoting language from *Griswold v. Connecticut*.[60] The quote was, "The First Amendment has a penumbra where privacy is protected from governmental intrusion."[61] The Court left many questions unanswered as to the source and scope of information privacy protection.

Despite the Court's distinction between information privacy and decisional privacy, law Professor Paul Schwartz wrote, "Decisional and information privacy are not unrelated; the use, transfer, or processing of personal data by public and private sector organizations will affect the choices that we make."[62] Gayle Horn of the Institute for

---

[57] *Id.* at 600.

[58] *Id*.

[59] *Olmstead*, 277 U.S. at 478.

[60] 381 U.S. 479 (1965).

[61] *Id.* at 483.

[62] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2058 (2004).

International Law and Justice at New York University described a "problematic" chilling effect that she said occurs when "individuals seeking to engage in lawful activity are deterred from doing so by a governmental regulation not specifically directed at that activity."[63] Despite the fact that they might be deciding to participate in many perfectly legal actions, such as visiting Muslim Websites, purchasing "adult" materials, donating to a racist organization, or ordering Viagra online, liberty may be lost as individuals consider the ramifications of having information regarding such choices added to their dossiers and made available to the government. As law Professor Jeffrey Rosen wrote, "[W]hen intimate information is removed from its original context and revealed to strangers, we are vulnerable to being misjudged on the basis of our most embarrassing, and therefore most memorable, tastes and preferences."[64]

Law Professor Stan Karas seemed to agree with Schwartz that informational and decisional privacy are interrelated and offered insight into why a chilling effect such as

---

[63] Gayle Horn, Note, *Online Searches and Offline Challenges: The Chilling Effect, Anonymity and the New FBI Guidelines*, 60 N.Y.U. ANN. SURV. AM.L. 735, 749 (2005); *see also* K. A. Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of Old King Ludd*, 7 YALE SYMP. L. & TECH. 123, 146 (2004/2005), http://research.yale.edu/lawmeme/yjolt/files/20042005Issue/6_Taipale121804Fx.pdf. He cites Roger Clarke in defining a chilling effect resulting from data mining as "the concern that potential lawful behavior, particularly constitutionally protected activity, would be inhibited due to the potential for a kind of post hoc surveillance (often referred to as dataveillance) that is said by many to result from the increased sharing of information among currently discrete sources.); *see* Clarke, *supra* note 1, at 498-512.

[64] JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 9 (2000); *see also* Arthur R. Miller, *Computers, Data Banks and Individual Privacy: An Overview, in* SURVEILLANCE, DATAVEILLANCE, AND PERSONAL FREEDOMS: USE AND ABUSE OF INFORMATION TECHNOLOGY 11, 19 (Columbia Human Rights Law Review Staff eds., 1972) (asserting many people had come to feel that their success or failure in life ultimately turned on what other people put in their file and an unknown programmer's ability—or—inability—to evaluate, process, and interrelate that information); *C.f.* Solove, *supra* note 9, at 1417-18 (arguing that the most insidious aspect of the surveillance is missing in the context of databases--human judgment about the activities being observed, that since marketers generally are interested in aggregate data they do not care about snooping into particular people's private lives, and since individuals are watched not by other humans, but by machines, this impersonality makes the surveillance less invasive); *see generally C.f.* Zarsky, *supra* note 5 (arguing that automated data processing is more equalitarian because various biases common among human analysts won't be part of the query and thus search results will be truly objective).

that described by Horn might occur. Karas described a power imbalance when he argued, "[T]he rationale behind the *Griswold* line of cases may be characterized as follows: intruding on private decisions is knowing, knowing is classifying, and classifying is impermissibly controlling."[65] Having knowledge about an individual's personal information is to have power over that individual. This notion is not new. In 1967 Professor Alan Westin wrote:

> The most serious threat to an individual's autonomy is the possibility that someone may penetrate the inner zone and learn his ultimate secrets, either by physical or psychological means. This deliberate penetration of the individual's protective shell, his psychological armor, would leave him naked to ridicule and shame and would put him under the control of those who knew his secrets.[66]

Stated another way, knowledge is power.

Solove once described information privacy law as "a mosaic of various types of law: tort law, constitutional law, federal and state statutory law, evidentiary privileges, property law, and contract law."[67] This dissertation is focused solely upon judicial conceptualizations of the constitutional right to information privacy, a protection that is only invoked when the government or an agent of the government infringes upon the right. The body of law regarding this requirement of government infringement is called

---

[65] Karas, *supra* note 25, at 426. He argued: "[P]ossessing information about an individual allows classification and exercise of discursive power over him or her.); s*ee also* Miller, *supra* note 64, at 13. "In a computerized society those who control the recordation and preservation of personal data will have a degree of power over the individual that is at once unprecedented and subject to abuse."

[66] WESTIN, *supra* note 20, at 33.

[67] SOLOVE, *supra* note 4, at 56.

the state action doctrine. Almost always, the state action doctrine is interpreted to exclude the actions of private persons, organizations, or businesses from constitutional scrutiny.[68]

The heavy involvement of the private sector in federal dataveillance challenges the existing state action doctrine. Robert O'Harrow, Jr., *Washington Post* reporter and associate of the Center for Investigative Reporting, noted: "It's a simple fact that private companies can collect information about people in ways the government can't. At the same time, they can't be held accountable for their behavior or their mistakes the way government agencies can."[69] Law Professor Neil Richards also warned, "To the extent that such private [data] collection is not state action, it allows the government, in effect, to outsource surveillance beyond the scope of otherwise applicable statutory and constitutional restrictions."[70] Determining whether the private companies that contribute to federal dataveillance are state actors is beyond the scope of this study. The analysis in this dissertation will focus solely on participation by the federal government in dataveillance programs.

In sum, many modern privacy protections are rooted in the Founders' notions of personal right and in the common law. The Supreme Court eventually recognized that a constitutional right to privacy exists in the penumbras and emanations of the Bill of Rights and later that each individual possesses a constitutional right to avoid the disclosure of personal matters to the government. The government's use of KDD

---

[68] Commonwealth of Virginia. v. Rives, 100 U.S. 313, 318 (1879). "The provisions of the Fourteenth Amendment of the Constitution we have quoted all have reference to State action exclusively, and not to any action of private individuals."

[69] O' HARROW, JR., *supra* note 3, at 8-9.

[70] Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1159 (2005).

technology for domestic surveillance in the name of national security represents a significant challenge for what can only be considered a nascent legal doctrine.

Scholarly debate has been ignited over the value of information privacy and how to balance society's interest in protecting that value against the federal government's need to conduct dataveillance in its counterterrorism efforts. A discussion of the significant privacy conceptualizations that have emerged in privacy scholarship is presented below and serves as the conceptual framework of this dissertation.

Conceptualizations of Privacy: A Review of the Scholarly Literature

This review of privacy scholarship[71] provides a conceptual framework for the following analysis of privacy case law and its eventual application to KDD. This section describes some of the principle conceptualizations of privacy that have emerged since Warren and Brandeis urged recognition of privacy rights beyond the private property interests protected by the Bill of Rights.[72] The term "conceptualization" is used to refer to a characterization that comprises either a statement of what a right of privacy is intended to protect (space, intimacy, information, etc.), a discussion of the societal and individual values that a privacy right safeguards (autonomy, self-government, reputation, etc.), or both.

[71] This literature review focuses on works discussing the conceptualizations of a constitutional right to privacy, the fundamental value of privacy in general, and information privacy. It does not discuss the growing body of public policy research that deals with implementation strategies for information technologies that promote civil liberties. Other literature not examined includes topics such as privacy torts, privacy policies/contracts, federal and state privacy statutes, and information ethics. There is also a large body of historical literature that might offer insight into the present national security posture. Nevertheless, those bodies of literature would not directly advance this query and are therefore excluded from this review.

[72] Warren & Brandeis, *supra* note 48.

Some of these conceptualizations are the original ideas of scholars and others originate in case law discussed by scholars. During the twentieth century, conceptualizations of privacy have gradually evolved from privacy as the right to a private, physical space to privacy as the right to control access to and the use of personal information. However, even today, as law Professor Anita Allen has asserted, "There is no universally accepted philosophical definition of 'privacy.'"[73] Professor Jerry Kang agreed, "Privacy is a chameleon that shifts meaning depending on context."[74]

Three major conceptualizations of privacy are discussed below: privacy as space, privacy as secrecy, and privacy as information control. Variations and major concepts associated with these conceptualizations are also discussed. Though no one conceptualization has succeeded in defining privacy in every context, they are all linked by one commonality;[75] each involves an individual's right to conceal, manipulate, or

---

[73] Anita L. Allen, *Privacy as Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 864 (2000).

[74] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN L. REV. 1193, 1202 (1998); *see also* Allen, *supra* note 73 (attributing the wide variation in definitional accounts of privacy to three factors: "(1) variation in the use and denotational and connotational meanings of privacy; (2) variation in the purposes for which the definition of privacy is undertaken; and (3) variation in approaches taken to the task of definition itself").

[75] A number of privacy scholars have grouped privacy conceptualizations by common elements in order to simplify their analysis or to discredit concepts contrary to their own. *Compare* JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 75-79 (1997) (recognizing three aspects of privacy: information privacy (control over information about oneself), accessibility privacy (limits on information and physical access that allow for seclusion), and expressive privacy (protects a realm for expressing one's self-identity or personhood through speech or activity"), *and* Kang, *supra* note 74, at 1202-05 (defining three "clusters" of privacy interests: space, decision, and information), *and* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1092 (arranging privacy conceptualizations into six groups for purposes of analysis: (1) the right to be let alone—Samuel Warren and Louis Brandeis's famous formulation of the right to privacy; (2) limited access to the self—the ability to shield oneself from unwanted access by others; (3) secrecy—the concealment of certain matters from others; (4) control over personal information—the ability to exercise control over information about oneself; (5) personhood—the protection of one's personality, individuality, and dignity; and (6) intimacy—control over, or limited access to, one's intimate relationships or aspects of life).

grant access to personal information. The conceptualizations are discussed in the order in which they emerged in the legal scholarship.

Privacy as Space

Under this conceptualization, privacy protections guard against physical or technological intrusion into some physical space by unwelcome third parties. The most common example of this conceptualization is the Fourth Amendment. Ratified in 1791 in the tradition of "a man's house is his castle," the Fourth Amendment protected the right of the people to be secure in their "persons, houses, papers, and effects,"[76] but it did so only against invasions by agents of the state, leaving citizens unprotected from invasions by private entities.[77] As legal analyst Irwin Kramer noted, "Consequently, the Fourth Amendment applied only to a small percentage of privacy invasions," and he asserted that it was dissatisfaction "with the lack of effective legal remedies available to those who found their privacy invaded, particularly those victimized by an overzealous and increasingly invasive press,"[78] that led Warren and Brandeis to write their famous law review article.[79]

---

[76] U.S. CONST. amend. IV.

[77] Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 30 CATH. U.L. REV. 703, 705 (1990).

[78] *Id*. at 709.

[79] *See also* Prosser, *supra* note 51 (asserting that Warren was motivated to write the article because of intrusive press coverage of his daughter's wedding); *C.f* . James Barron, *Warren and Brandeis,* The Right to Privacy, *4 Harv. L. Rev. 193 (1890): Demystifying a Landmark Citation,* 13 SUFFOLK U.L. REV. 875 (1979) (explaining that Warren's annoyance could not be about his daughter's wedding as she was only ten years old in 1890); *see also* SMITH, *supra* note 16, at 121 (suggesting it was the "cumulative impact of intrusive reporting by the press over the years" that caused Warren's outrage).

By 1890, when the Warren and Brandeis article was published, the Supreme Court had interpreted the Fourth Amendment as a private property right intended to prevent the government from using general warrants to search tangible space such as one's home for criminal evidence to be used against citizens.[80] Nevertheless, Warren and Brandeis not only conceived of privacy as a protection of a private space but also as an individual's broader right to be left alone.[81] They thought a person should be able to step out of the public sphere and claim sanctuary in a private space.

Smith noted that "each time there was a renewed interest in protecting privacy it was in reaction to new technology."[82] Between 1870 and 1890 great advances were made regarding sound recording, telephony, and instant photography, and these technologies made it much easier for private entities such as the press to invade private homes. Warren and Brandeis warned, "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[83] The pair sought to expand individuals' privacy interests to include intangible property, such as their thoughts or emotional wellbeing, which were being threatened by these "recent" inventions.

---

[80] *See* Boyd v. United States, 116 U.S. 616, 630 (1889). "Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods, is within the condemnation of that judgment. In this regard the Fourth and Fifth Amendments run almost into each other."

[81] Warren & Brandeis, *supra* note 48.

[82] *Id.*

[83] *Id*. at 195.

According to Warren and Brandeis, the value that they believed should be protected by privacy law was one's "inviolate personality."[84] They argued that private physical space was necessary to protect intangible privacy interests such as one's emotional wellbeing, and this interest was not recognized by the law at that time. They wrote, "The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual."[85] Alan Westin described this as a need for a "back stage area" because no individual can "play indefinitely, without relief, the variety of roles that life demands" while interacting in public.[86]

This line of reasoning frames privacy law as a means to protect an individual's emotional well-being against harms that would result from the loss of one's private space. As Cohen explained, "The injury, here, does not lie in the exposure of formerly private behaviors to public view, but in the dissolution of the boundaries that insulate different spheres of behavior from one another."[87] Professor Amatai Etzioni ascribed a societal value to a protected legal space. He wrote that in order for an individual to fulfill a public role, a "societal license that exempts a category of acts (including thoughts and

---

[84] *Id*. at 205.

[85] *Id*. at 195.

[86] WESTIN, *supra* note 20, at 35-36. He went on to note that on any given day a man may move through the roles of a stern father, loving husband, carpool comedian, skilled lathe operator, union steward, water cooler flirt, and American Legion Committee Chairman—all psychologically different roles that he adopts as he moves from scene to scene on the social stage; *see also* Charles Fried, *Privacy* 77 YALE L. J. 475, 477 (1968) (asserting that private space was necessary as "a context for respect, love, friendship, and trust" which is why "a threat to privacy seems to threaten our very integrity as persons" and thus tying the spatial concept of privacy to personhood).

[87] Cohen, *supra* note 25.

emotions) from communal, public, and governmental scrutiny" must be provided.[88] Etzioni argued that the preservation of individual privacy should be a social priority.

Schwatrz agreed with Etzioni. He wrote, "Rather than on a right of control, the focus of information privacy law should be construction of a privacy space that promotes civil society and individual decision making."[89] In this way, private space might be considered vital to the success of a democracy. Westin explained the connection between the preservation of private space and the promotion of civil society as a need for "individuality" when he wrote:

> This development of individuality is particularly important in democratic societies, since the qualities of independent thought, diversity of views, and non-conformity are considered desirable traits for individuals. . . . The independence necessary for participation in self-government requires time for sheltered experimentation and testing of ideas, for preparation and practice in thought and conduct, without fear of ridicule or penalty.[90]

Thus, Westin argued that development of individuality was necessary for the sound decision making that promotes a civil society. Others have argued that it is the development of autonomy that is the societal value of maintaining private spaces.

For example, Cohen wrote, "Development of the capacity for autonomous choice is an indispensable condition for reasoned participation in the governance of the community and its constituent institutions -- political, economic, and social."[91] Using

---

[88] AMITAI ETZIONI, THE LIMITS OF PRIVACY 196 (1999) (suggesting that a sound communitarian treatment of privacy views it as the realm in which the actor--a person, a group, or a couple--can legitimately act without disclosure and accountability to others).

[89] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1677 (1999).

[90] WESTIN, *supra* note 20, at 34.

[91] Cohen, *supra* note 25, at 1426; *see also id.* (asserting that autonomy in a contingent world requires a zone of relative insulation from outside scrutiny and interference—a field of operation within which to engage in the conscious construction of the self).

similar reasoning to Westin's, Cohen argued that a functioning democracy requires intellectual autonomy and that private space provided "the freedom to explore areas of intellectual interest that one might not feel as free to explore in public."[92] It is this intellectual exploration that leads to an informed populace capable of self-government.

If the barrier between one's private and public spheres is eroded by surveillance, there is a danger of self-censorship. Cohen wrote: "[T]he experience of being watched will constrain, ex ante, the acceptable spectrum of belief and behavior. Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and mainstream."[93] Schwartz called this pressure to conform the "coercive standardization of the individual . . . when private or government action interferes with a person's control of her reasoning process."[94] Self-censorship may thus impede the formation of autonomous individuals, which is so important to self-governing societies.

Smith defined privacy as "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves."[95] His definition is notable for two reasons. First, he incorporated information privacy within the spatial concept of privacy. Smith asserted that one reason to protect a private space was to facilitate the control of information. Second, he recognized "harms" in his definition. Smith noted that one might suffer embarrassment or accountability if others

---

[92] Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L. J. 575, 579 (2003). She wrote that private space "also affords the freedom to dictate the circumstances—the when, where, how, and how often—of one's own intellectual consumption, unobserved and unobstructed by others."

[93] Cohen, *supra* note 25, at 1426.

[94] Scwartz, *supra* note 89, at 1654-55.

[95] SMITH, *supra* note 16, at 6.

had knowledge of what was occurring behind closed doors or written within sealed envelopes.

In sum, the privacy-as-space conceptualization involves the maintenance of both a private and public sphere of existence for each individual. Individuals value this zone of privacy because it facilitates the intellectual and emotional exploration necessary for the development of autonomous individuals. The existence of this space also has a societal value, the maintenance of an informed populace capable of self-government. Self-censorship for fear of potentially negative ramifications from third-party knowledge of certain behaviors may result from an invasion or dissolution of this private space.

Privacy as Access to Self

A variation of the privacy-as-space conceptualization is privacy as access to self. Under this conceptualization, space in the sense of land, a dwelling, or a file drawer was no longer the sole concern. Rather, one's "self" was conceptualized as the zone of privacy. The self is one's personality, thoughts, beliefs, intellect, body, and bodily fluids. Thus, privacy as access to self may be invoked to protect against a body cavity search or a urinalysis test. It also might protect against having a love letter read aloud, having political contributions disclosed, or having law enforcement personnel access one's library records. This privacy conceptualization is reflected in Brandeis's 1928 dissent in *Olmstead*. The information being intercepted in the telephone wires could provide law enforcement with a glimpse into the speaker's personality, a violation of privacy as access to self.

A number of scholars have conceptualized privacy in this way. Sociology professor Stephen Nock wrote: "Privacy results from the legitimate denial of access to one's actions or records. Privacy is defined by the socially-recognized legitimate right to restrict others from observing or knowing about one's actions."[96] Professor Ruth Gavison also discussed this conception of privacy when she wrote, "Our interest in privacy . . . is related to our concern over our accessibility to others, the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of other's attention."[97] Rosen has argued for a more prominent role for privacy as access to self in privacy jurisprudence. Referring to *Roe v. Wade,*[98] Rosen opined:

> [B]y focusing on an amorphous vision of privacy that is really a misnomer for the freedom to make intimate decisions about reproduction, the Supreme Court has neglected a more focused vision of privacy that has to do with our ability to control the conditions under which we make different aspects of ourselves accessible to others.[99]

This concept is still ultimately about an individual's right to maintain a zone of privacy. However, it can be distinguished from the spatial privacy conceptualization because the zone does not need to be anchored to a physical location. It is anchored in one's personality or identity or body. As noted above by Horn and Karas, government knowledge about intimate decisions could ultimately lead to a chill in certain activities

---

[96] STEPHEN L. NOCK, THE COSTS OF PRIVACY, SURVEILLANCE AND REPUTATION IN AMERICA 11-12 (1993); *see also* WESTIN, *supra* note 20 (defining privacy as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others).

[97] Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L. J. 421, 423 (1980); *id.* at 428. Gavison defines a loss of privacy as occurring as "others obtain information about an individual, pay attention to him, or gain access to him."

[98] 410 U.S. 113 (1973).

[99] ROSEN, *supra* note 64, at 15.

despite the legality of the actions in question. Like the spatial concept of privacy, privacy as access to the self is primarily concerned with a zone of privacy, information flow, and the avoidance of a chill.

Privacy as Secrecy

Solove has dubbed the collection of privacy conceptualizations that are predicated upon the obligation of individuals to define their own private space the "secrecy paradigm."[100] Sometimes referred to as the third-party doctrine, this conceptualization assumes a societal presumption toward disclosure rather than privacy. Under the secrecy paradigm, only information that is consciously hidden from others will be considered private.[101] Solove described infringement under the secrecy paradigm this way: "[P]rivacy is invaded by uncovering one's hidden world, by surveillance, and by the disclosure of concealed information . . . . [I]f the information isn't secret, then courts often conclude that the information can't be private."[102] The value to be served by privacy protections under the secrecy paradigm is the protection of individuals from harms brought about by the use of personal information by third parties.

---

[100] SOLOVE, *supra* note 4, at 8. Also called the third-party doctrine, this phrase was coined by Solove and refers to the bedrock principle in American privacy law that information shared with another, or made part of the public record, can no longer be private. Solove argues this paradigm is no longer valid in a society were it is "virtually impossible to live as an information age ghost, leaving no trail or residue."

[101] *See* Katz v. United States, 389 U.S. 347, 351 (1967). "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected;" *Id*. at 362 (Harlan, J., concurring). "[C]onversations in the open would not be protected against being overheard . . . . The critical fact in this case is that '(o)ne who occupies it (a telephone booth) shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume' that his conversation is not being intercepted;" Smith v. Maryland, 442 U.S. 735, 743-44 (1970). "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."

[102] SOLOVE, *supra* note 4, at 8.

According to Smith, a number of cultural changes after World War II created a "mania for personal information gathering." These changes included an increased use of credit coupled with a mobile population that could not be serviced by local credit bureaus, mandatory state drivers' insurance, and broader adoption of medical insurance, and, as noted above, the rapid increase in the number of governmental programs that required qualifying information.[103] When the Founders drafted the Fourth Amendment, privacy was valued as a check on federal power. When Warren and Brandeis argued for legal protections for private space, privacy was threatened by invasive new technologies and valued as necessary for the development of individuals capable of self-government. The secrecy paradigm originated at a time when society needed access to personal information in order to function, and this need conflicted with individual privacy rights in personal information.

Modern scholars recognize that the privacy-as-secrecy conceptualization has influenced information privacy law. Privacy expert Anita Allen suggested: "Informational privacy obtains where information actually exists in a state of inaccessibility, whether it is locked in a file drawer, computer, or in someone's mind. Anonymity, confidentiality, reserve, and secrecy—not merely having the choice to bring these about—are forms of privacy."[104] Nevertheless, some argue that new information technologies make the conceptualization unworkable.

An important idea in privacy-as-secrecy scholarship is that of limited privacy, which was defined by Professor Lior Strahilevitz as "the idea that when an individual

[103] SMITH, *supra* note 16, at 313-14.

[104] Allen, *supra* note 73, at 868-69.

reveals private information about herself to one or more persons, she may retain a reasonable expectation that the recipients of the information will not disseminate it further."[105] For instance, a person might inform his family members during dinner that he lost his job and assume that they will not reveal that information beyond their small circle of intimates. Relationships such as patient-physician and lawyer-client are examples of situations in which the law clearly protects such limited privacy.

The notion of limited privacy is especially important when considering the potential harms associated with digital dossiers and KDD technologies. In regard to databases, Solove argued that "information about an individual . . . is not often secret, but is diffused in the minds of a multitude of people and scattered in various documents and computer files across the country."[106] As discussed above, it is necessary for people to share information in order to function normally in society, but, as asserted by Solove, "individuals want to keep things private from some people but not from others."[107] Law professor Stephen Henderson explained how the nature of database construction necessarily erodes the applicability of the privacy-as-secrecy conceptualization. He argued:

> [T]he third party doctrine . . . becomes especially suspect when one considers the extraordinary databases under construction today. Whether one should be considered to have affirmatively given information to a third party for use when that information is incorporated into a database of entirely unforeseeable scope and intent is not clear.[108]

---

[105] Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy,* 72 U. CHI. L. REV. 919, 939 (2005).

[106] SOLOVE, *supra* note 4, at 42-43.

[107] *Id.* at 43-44.

[108] Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV.507, 548 (2005).

Henderson argued that a key problem with the secrecy paradigm or third-party doctrine was that it "treats privacy as an indivisible commodity."[109] Once individuals surrender information, it is assumed they have given up all control over the use and dissemination of it. Instead, Solove argued: "We must . . . recognize that what is public can be private—not in the sense that it is secret, but in that uses and disclosures of information can be limited. Privacy is about degrees of accessibility."[110]

KDD complicates matters because it creates knowledge that was never surrendered at all. For instance, an individual might voluntarily surrender bits of information such as which grocery items he purchases using a discount savings card at a local store, but can it be assumed that he knowingly surrendered the insights into his life that analysts are able to derive from the raw transaction data? Technology columnist Dr. Joseph Fulda identified the problem with applying the privacy-as-secrecy conceptualization to information discovered following KDD analysis. Fulda asked, "Is it possible for data that does not in itself deserve legal protection to contain implicit knowledge that does deserve legal protection?"[111] It stands to reason that individuals are not able to choose to conceal knowledge that does not preexist. Fulda argued, "[T]he old legal rule that anything put by a person into the public domain is not legally protected served well when the data was not mined so as to produce classifications, clustering,

[109] *Id*. at 546 (2005).

[110] Solove, *supra* note 23, at 1217-18.

[111] Joseph S. Fulda, *Data Mining and Privacy*, 11 ALB.L.J. SCI. & TECH. 105109 (2000); *see also* Tien, *supra* note 30, at 409 (asserting that the proper response to the obstacle posed by the "knowing exposure" doctrine is that the underlying patterns or associations are not the same as the surface facts in a database and that these patterns may themselves be private).

summaries, and profiles, dependencies and links, and other patterns."[112] This is the primary problem, Solove argued, with using the popular Big Brother metaphor for describing federal dataveillance.[113]

Solove wants to retire the secrecy paradigm and the Big Brother metaphor. He has argued for a new metaphor based on the work of novelist Franz Kafka. He wrote:

> Privacy law has developed with [the secrecy] paradigm in mind, and consequently, it has failed to adapt to grapple effectively with the database problem . . . . I argue that the problem is best captured by Franz Kafka's depiction of bureaucracy in *The Trial*—a more thoughtless process of bureaucratic indifference, arbitrary errors, and dehumanization, a world where people feel powerless and vulnerable, without any meaningful form of participation in the collection and use of their information.[114]

This describes a different power imbalance than that asserted by Karas regarding a potential for self-censorship when the government can access information regarding the intimate decisions in one's life. Solove feared the imbalance that emerges when individuals are at risk because they cannot access or control information held by large bureaucracies.[115]

---

[112] Fulda, *supra* note 111, at 108. Fulda goes on to argue that so much of an individual's personality, or likeness, is revealed by KDD processes that such new knowledge is protected by the tort of appropriation. He does not attempt to define a constitutional right to informational privacy.

[113] Solove, *supra* note 9. Big-Brother is the totalitarian government in George Orwell's novel *1984*. Citizens were always being watched by the government through view screens. This metaphor is often used when discussing domestic surveillance.

[114] *Id*. at 1398 (2001).

[115] *See* SMITH, *supra* note 16, at 315. Smith explains that historically the individual did not have the knowledge or funding to access or manage personal data held by third parties. He noted, "Between the 1950s and the 1980s, the early days of computing, only the government bureaucracies, colleges and universities, labor unions, corporate employers, national banks, and insurance companies had the resources to own computer systems;" *see also* BRIN, *supra* note 40, at 253 (claiming that the aim of privacy is to end asymmetries or inequities in the flow of information and then let market forces drive the result and also that today, despite cheaper technology and the increase in computer literacy among the population, few individuals have mastered the complex level of programming necessary to understand technologies like KDD).

In summary, since the mid-twentieth century life in the United States has required the surrender of personal information. Privacy law reflected that new societal priority when it adopted the privacy-as-secrecy conceptualization, which stripped away privacy protections for any information shared with a third party, placed the burden of protecting privacy on the individual, and placed people at risk of being misjudged on incorrect information they could not access to correct.

Privacy as Information Control

The massive growth of direct marketing and the resulting emergence of the data industry in the 1990s created both an individual and societal interest in being able to control one's personal information. It was during this decade that there was a renewed interest in privacy conceptualizations that would influence the courts to shift the focus of information privacy law away from a fundamental right to conceal or hide personal information to a fundamental right to control personal information.

This conceptualization, as Solove wrote, "entails control over and limitations on certain uses of information, even if the information is not concealed."[116] David Brin wrote that "if the information contained in [a] system was made available against an individual's wishes or if that information were obtained without consent we could speak of a violation of that person's privacy."[117] Schwartz defined privacy as "a personal right

[116] Solove, *supra* note 23, at 1178.

[117] NOCK, *supra* note 96, at 13.

to control the use of one's data,"[118] and Allen, while critiquing Schwartz's definition, recognized three separate elements of privacy as information control. She wrote:

> They are, first, the notion that the term "privacy" means control (or rights of control) over the use of personal data or information; second, the notion that the expression "right to privacy" means the right or claim to control the use of personal data or information; and, third, the notion that the central aim of privacy regulation should be promoting individuals' control (or rights of control) over personal data or information.[119]

Schwartz understood the information-control conceptualization to provide individuals with a bundle of privacy rights with which to protect their personal information.[120] The conceptualization presumes that one may access previously shared information, may exert control over secondary uses of that information, and may determine the degree or type of information shared. Solove considered secondary uses of personal information that had been compelled by government and then sold to private companies especially troubling. He wrote that the information in "public records is often supplied involuntarily and typically for a purpose linked to the reason why the particular records are kept. The problem is that, often without the individual's knowledge or consent, the information is then used for a host of different purposes by both the government and businesses."[121] Since 9-11 this trend is occurring in the opposite direction as well. Information voluntarily given to private companies and organizations is being accessed and used by government to discover new knowledge.

---

[118] Paul M. Schwartz, commentary, *Internet Control and the State*, 32 CONN.L. REV. 815, 816 (2000).

[119] Allen, *supra* note 73, at 863.

[120] Schwartz, *supra* note 62, at 2094.

[121] Solove, *supra* note 23, at 1194-95.

A major idea regarding privacy as information control is that privacy protections can function as elements of social architecture. In 1968 Professor Charles Fried pondered whether a man alone on an island had privacy. He wrote, "Privacy is not simply an absence of information about us in the minds of others, rather it is the control we have over information about ourselves."[122] Fried ultimately decided the man had no privacy because he had no opportunity to grant or deny access to information to others. His example demonstrates that a privacy right can only exist in a relationship and that the level of protection provided the right equals a measure of power within that relationship.

To the extent that privacy protections, through an allocation of power, structure relationships, they function as agents of social architecture.[123] Solove wrote:

> Privacy involves the power to refuse to be treated with bureaucratic indifference when one complains about errors or when one wants data expunged. It is not merely the collection of data that is the problem—it is our complete lack of control over the ways it is used or may be used in the future.[124]

Thus the value of privacy as control of information is its ability to bolster individual sovereignty relative to the entities controlling the new information technologies.

In 1999 Lawrence Lessig was writing about how to apply constitutional values in cyberspace. His central contention was that the computer code used to structure virtual space should be written to support and advance American culture's most sacred values such as free speech and privacy rights. In this way Lessig conceived of computer code as social architecture. Lessig wrote, "I mean an architecture—not just a legal text but a way

---

[122] Fried, *supra* note 86, at 482.

[123] *See* Solove, *supra* note 32, at 1116. Conceived of in this way, privacy is a form of freedom built into the social structure and about the common good as much as it is about individual rights.

[124] Solove, *supra* note 9, at 1426.

of life—that structures and constrains social and legal power to the end of protecting fundamental values, principles, and ideals that reach beyond the compromise of ordinary politics."[125] Solove saw privacy law in a similar way, as an architecture that built freedom into the American social structure. He asserted:

> Protecting privacy through an architecture of power differs from protecting it as an individual right. The problem with viewing rights in purely individualistic terms is that it pits individual rights against the greater good of the community, with the interests of society often winning out because of their paramount importance when measured against one individual's freedom. [126]

Solove further suggested, "The [privacy] architecture's scope should encompass all instances where third parties share personal information contained within a system of records . . . [and] should focus on at least two sets of relationships: relationships with government and relationships with the third parties that possess personal information."[127]

Ideally then, the privacy-as-information-control conceptualization should empower individuals by allowing them to structure their own relationships with third parties holding their personal information. For instance, when consumers shop online they are usually prompted to read a Website's privacy policy, evaluate how the Website will collect and use the data supplied, and then make an informed decision as to whether to share personal information. When individuals are empowered to negotiate privacy terms on their own, without assistance from the government, it can be said that an information marketplace exists and is functional. If the marketplace is functioning

---

[125] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 5 (1999).

[126] Solove, *supra* note 32, at 1156.

[127] *Id*.

properly, then individuals will protect their privacy interests without assistance from government. Conversely, the market failure critique put forth by some scholars assumes that certain social realities will interfere with the marketplace functions unless the government interferes.[128]

Anita Allen alluded to one type of market failure when she wrote: "Having control over personal information does not mean having privacy. The person in control of her data might elect to share personal information with others."[129] If the Court were to recognize a fundamental value to society in individual control of personal information, then the government would need to convince individuals not to give away information haphazardly or pass laws that make it difficult for third parties to utilize personal information without the consent of the individuals to whom the data pertain.

Another possible type of market failure is that few individuals may have the capacity to track their information once they initially surrender it. Large businesses and government agencies are capable of building digital dossiers, sharing them among different databases, and using KDD technologies to develop new information about the subject. Individuals generally are not able to understand these systems and cannot manage the use or sharing of their personal information. As Allen wrote, "It is pointless (or merely symbolic) to ascribe a right to data control if it turns out that exercising the right is impossible."[130]

---

[128] *See generally* C. Edwin Baker, *Scope of the First Amendment Freedom of Speech* 25 UCLA L. REV. 964 (1977-1978) (providing a market failure critique to classic First Amendment marketplace theory).

[129] Allen, supra note 73, at 867; *id*. at 871 (calling privacy irresponsible because laws designed to give individuals more control over their personal information will not work because people will "use the rights of data control to give up forms of privacy deemed vital to their interests").

[130] *Id.* at 869.

In sum, scholars see a privacy-as-information-control conceptualization as more effective than the secrecy paradigm when applied to massive databases and KDD technology. Conceived of as information control, information privacy protections empower individuals to control access to and use of their personal information. To the extent that a right to information privacy allocates power, it structures relationships. Thus, information privacy protections are elements of social architecture and even economic architecture. The market failure critique, when applied to the privacy-as-information-control conceptualization, posits that people will not be able to control their personal data without government support because individuals often give away their personal information or are incapable of controlling it.

Privacy as Property

One variation of the privacy-as-information-control conceptualization is the privacy-as-property conceptualization. Some scholars, such as Richard Murphy, take the view that "personal information is in fact, property."[131] This conceptualization differs from the private property concept discussed relative to the Fourth Amendment because here individuals have a property right in information that can be traded – not in physical space. For example, Professor Eugene Volokh noted that one can argue for property rights in personal information "on functional grounds: Those who communicate personal information about others are engaging in a sort of free riding, enriching themselves without compensating the people whose existence makes their enrichment possible; and

[131] Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L. J. 2381, 2393 (1996).

property rights, the argument goes, are the way to avoid this free riding."[132] Like the secrecy conceptualization, the property conceptualization assumes individual agency in defining which information is to remain private.

Understanding privacy as a property right presupposes ownership of two assets: the privacy right itself (my privacy) and personal data (my information). Here privacy law protects an individual's right to negotiate the terms of sale, trade, or surrender of personal data. As does the privacy-as-information-control conceptualization, the privacy-as-property conceptualization can empower individuals relative to large bureaucracies.

When applied to the privacy-as-property conceptualization, a market failure critique would highlight that there is no guarantee that individuals will use property rights in their personal information in a manner that benefits themselves or society. Professor Michael Froomkin referred to the tendency of people to "sell their data too often and too cheaply" as "privacy myopia."[133] The popularity of participating in reality TV, live webcams, and blogs might indicate that one's fleeting fame is more enticing than the maintenance of a private zone for the facilitation of intellectual and spiritual self-development.

Another market failure critique is that when privacy is conceptualized as a tradable property right, it should not be assumed that information transactions will take place between two equal partners. Individuals with more technological savvy, more education, more experience, or insight into how information is managed may be better able to leverage their personal information. These disparate levels of social power will

---

[132] Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1073-74 (2000).

[133] *See* Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1502, 1505 (2000).

reveal a disparity in what Tal Zarsky, a resident fellow in the Information Society Project at Yale Law School, described as "sophistication." He wrote:

> In today's technological reality, equal access to information is insufficient, and access to raw data is almost as good as having no access to data at all. To grasp and analyze the vast amounts of information available, sophistication is now the key . . . . [D]ata mining applications are expensive and at times beyond the reach of the general public . . . . Should such uneven access persist in a transparent society, transparency will in fact increase the disparity between individuals and large entities, rather than level the information playing field.[134]

In this passage Zarsky was critiquing the notion of a transparent society as proposed by best-selling science fiction author David Brin. Brin argued that the Big Brother domestic surveillance scenario could be diffused if individual citizens were technologically empowered to conduct surveillance on government and big business. Zarsky recognized that those with less education and fewer resources would be disadvantaged in such a system. Cohen agreed and described this scenario:

> Under a regime of tradable privacy rights, "privacy" simply will become a status that can be chosen (and paid for) the way one might choose a neighborhood, a health club, or a brand of automobile . . . . A perverse consequence of a purely market-based approach to data privacy rights, then, may be more discounts for the rich. If so, then the poor will lose twice over. They will have less privacy, and they will also pay more for goods and services than more desirable customers.[135]

Control under the privacy-as-property conceptualization can be exercised in two ways. First, individuals can treat their privacy as if it were an "indivisible

---

[134] Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. MIAMI L. REV. 991, 1022-23 (2004).

[135] Cohen, *supra* note 25, at 1398.

commodity."[136] This all-or-nothing approach means that people may trade away all their personal information and all rights to control what is done with that information at one time and in one transaction. The second way to exercise property rights in personal information is for individuals to use what Schwartz calls inalienabilities.

An inalienable property right is a restriction placed on someone who is using or holding your property.[137] For instance, one might rent a room to a student with the restriction, or inalienability, that the student not sublet the room to anyone else. With regard to personal information, inalienabilities might include restrictions such as third parties may not share personal data without one's consent, third parties may not use the data for direct marketing purposes, or third parties may not share personal information with law enforcement without providing notice to those whose data are being accessed.

Schwartz wrote, "In the context of personal data trade, a single combination of these inalienabilities proves to be of greatest significance - namely, a restriction on the use of personal data combined with a limitation on their transferability."[138] Schwartz suggested that by identifying a number of inalienabilities and understanding the privacy-as-property conceptualization as "a bundle of rights rather than despotic dominion over a thing" will help frame "a viable system of rights with respect to personal data."[139]

---

[136] Henderson, *supra* note 108, at 546.

[137] BLACK'S LAW DICTIONARY 774 (8th ed. 2004).

[138] Schwartz, *supra* note 62, at 2098.

[139] *Id.* at 2094; *see also* Cohen, *supra* note 25, at 1391 (asserting that current systems for processing transactions are designed to facilitate a one-time surrender of control over personal information, but they need not be because systems can be designed to make information privacy ownership "sticky" and efficient and that the design of such systems is a matter of choice).

Law Professor Andrew McClurg argued against the privacy-as-property conceptualization from a pragmatic position. He noted that the government does not generally recognize a property interest in mere information.[140] McClurg warned that if true property rights were to be recognized in personal facts, an entirely new doctrine of intellectual property would need to be established, and from both a practical and substantive perspective, this would be very difficult.[141] For example, even if the government supported property rights in individual facts, the problem would then shift to ownership of information revealed through the use of KDD technologies. In order to create such knowledge, a computer program has to be written and used to compile and organize that data. Some entity must provide the time, equipment, and expertise needed to build the dossier. Such entities may have valid legal grounds to argue ownership rights in discovered knowledge.

Fulda suggested that privacy protects reputation, and he argued for attaching property rights to reputation.[142] This avoids the "no property rights in mere information" problem by presuming that facts alone have no value, but, instead, it is the information derived from the facts that does.[143] One difficulty with Fulda's suggestion is that individuals would need to be able to know what knowledge was derived from their data, when, for what purpose, and by whom. Only if third parties are obligated by law to keep

---

[140] McClurg, *supra* note 24, at 92.

[141] *Id.* "A substantial infrastructure would be necessary to implement a property rights-based system of consumer data."

[142] *See generally* Joseph S. Fulda, *Reputation as Property*, ST. CROIX REV. 33, April 2000, at 30.

[143] Karas, *supra* note 25, at 424. "[I]t is important to note that privacy law and scholarship seek to protect not mere information relating to a person, but rather 'information plus,' information that is expressive of one's self."

individuals informed as to what information is being mined from their digital dossiers will placing a property interest in reputation offer reliable protection of information privacy.

The privacy-as-property conceptualization differs from the original concept of privacy under the Fourth Amendment because here privacy is conceptualized as a tradable property right. The property model empowers individuals and therefore structures relationships within society. It also provides a context in which information transactions can occur. Scholars have criticized this model for being unworkable. Market failure critiques such as individual neglect of property rights, unequal partners to a transaction, and failure of the government to recognize property rights in facts alone all weaken this conceptualization. Some scholars like Fulda and Schwartz have suggested solutions to these problems such as the use of inalienabilities and privacy rights in reputation.

Privacy as Contract

A second variation of the privacy-as-information-control conceptualization is the privacy-as-contract conceptualization. A privacy-as-contract conceptualization would empower individuals to utilize contracts to negotiate disclosure. Ideally a privacy contract would outline exactly what control each of the parties has over the data in question. This conceptualization would also establish a fundamental privacy default rule, which means that in all cases companies holding personal information would be forced to disclose how they make the information available to the government, and whenever information contracts are unclear the courts will interpret the contract to prevent the disclosure of the

plaintiff's personal information. The opposite of a privacy default is a disclosure default. A system with a disclosure default would interpret disputed contracts to allow access to and use of the information in question.

Richard Murphy defined the basic principle of the privacy-as-contract[144] paradigm: "Because information is voluntarily disclosed, there is no reason both sets of consumers cannot be satisfied through a contracting process."[145] Nevertheless, like the property model, the contract model requires a rather extreme cultural shift to be effective. America would need to adopt a privacy default standard as opposed to a disclosure default. Privacy expert Charles Sykes outlined how America might be transformed into a culture and society that respects privacy. He explained:

> We can begin to give individuals that control by creating a presumption of privacy as the default setting of the Information Age. Our presumption of privacy should be as strongly held—and jealously guarded—as our presumption that we have free speech, freedom to worship, the right to own private property, and equality of opportunity, all values that are deeply ingrained in our culture, law, and politics. In the case of the presumption of privacy, the burden should be on others to say why they have any right to know about our lives. Absent that, the presumption should be that each of us has control over such information. In practical terms that means that we should not be required to "opt-out" of a system that invades our privacy; the presumption of privacy would dictate that no one is allowed onto our zone of privacy without our specific choice to "opt-in."[146]

Under Sykes' paradigm, the courts would assume that in all circumstances individuals have a fundamental right to information privacy instead of disclosure and that individuals must "opt-in" to any disclosure contracts. An opt-in information market

[144] This conceptualization is sometimes called the privacy-as-choice concept.

[145] Murphy, *supra* note 131, at 2406.

[146] SYKES, *supra* note 22, at 246.

would mean that individuals must initiate any transaction that involves sharing their personal information. An opt-out information market is the opposite. Third parties could simply use personal data until they were asked to stop. An opt-in information market would empower individuals relative to the third parties that hold their personal data. Murphy wrote, "[A] privacy default rule, by forcing the seller to contract out, could generate more dynamic benefits and be less costly than a disclosure rule, even in a situation where only a minority prefers privacy to disclosure."[147]

Cohen commented that the privacy-as-contract conceptualization recognized what, for her, is the primary value in a privacy right, promoting the development of the autonomous self. Cohen wrote, "[A] market model of tradable privacy rights is fully consistent with first-order normative commitments to dignity and equality, in that it treats each individual as an autonomous, rational actor and presumes that all individuals are equally capable of ascertaining and pursuing the goals that will maximize their own happiness."[148]

Nevertheless, Cohen provided a market failure critique. She wrote that the contract model "presumes both the ability and the desire to alienate personal information (on the right terms), and thus devalues the argument that ownership necessarily includes the right to assert ongoing control."[149] Stated another way, the privacy-as-contract conceptualization assumes that individuals want to exercise ongoing control over their personal information, but there is a good chance people will not know how to do this or want to do this. To the extent that individuals contract away their right to ongoing control

[147] Murphy, *supra* note 131, at 2416.

[148] Cohen, *supra* note 25, at 1424.

[149] *Id.* at 1393.

to third parties, the privacy-as-contract conceptualization will be an ineffective information privacy protection.

In another market failure critique, Tal Zarsky noted that many individuals do not truly understand how their personal information will be used by third parties even if they read privacy policies and the terms of privacy contracts. He said individuals sign off on privacy polices without fully understanding the terms of the contract in question – what he called the "autonomy trap."[150] Individuals believe they are determining how their information will be used, but they are really unequal parties to the agreement because they don't know enough about private-sector and government use of personal information to make informed decisions regarding the terms of privacy contracts.

Professor Volokh, a prolific supporter of the privacy-as-contract conceptualization, argued the extreme position that contracts are the only information privacy protections that do not violate the free speech protections of the First Amendment. Volokh wrote:

> The difficulty is that the right to information privacy—my right to control your communication of personally identifiable information about me—is a right to have the government stop you from speaking about me. We already have a code of "fair information practices," and it is the First Amendment, which generally bars the government from controlling the communication of information (either by direct regulation or through the authorization of private lawsuits), whether the communication is "fair" or not. While privacy protection secured by contract is constitutionally

[150] *See generally* Zarsky, *supra* note 5, at § C ¶1. He explained the concept of the "autonomy trap," which asserts that even though individuals can make privacy choices regarding posted privacy policies, they are controlled by those collecting the information. He argued that the answer to the autonomy trap is a massive public opinion campaign that might prepare citizens to see around the choice limitations and avoid faux choices. He wrote, "The public, when aware of privacy concerns, could reduce the amount of personal data it provides collectors with, and insist on proper compensation when they choose to submit such information. In addition, people might apply general caution toward any feedback they receive from various content providers and advertisers, knowing that it might have been tailored especially for them."

> sound, broader information privacy rules are not easily defensible under existing free speech law.[151]

Schwartz responded to Volokh's argument and warned that "[b]y constitutionalizing out of existence privacy protections found in many legal sources, Volokh uses the First Amendment to set the stage for a reign of contract."[152] He argued that exclusive reliance on the privacy-as-contract model vests too much power in the individual. Because of a lack of technical knowledge and resources, individuals will be at a distinct disadvantage when sitting at a bargaining table with large private or government entities interested in getting their personal data.

Another problem noted by Schwartz is the role played by the courts in a strict privacy-as-contract paradigm. He pointed out: "One problem is that this reading of the First Amendment [as making privacy protections unconstitutional] would transform federal judges into arbiters with the power to decide if there existed a social convention of confidentiality that merited inclusion in the First Amendment's contract exemption."[153] Judges would be deciding whether an implied right of privacy existed in a contract between two parties within a given social context.

Conclusion

This review of privacy scholarship covered three broad conceptualizations of privacy. First, the privacy-as-space conceptualization was discussed. Originally

---

[151] Volokh, *supra* note 132, at 1050-51.

[152] Paul M. Schwartz, *Free Speech v. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV.1559, 1568 (2000).

[153] *Id.* at 1569.

grounded in Fourth Amendment protections for private property, spatial privacy broadened to include privacy-as-access-to-self, which protected intangible interests such as one's inviolate personality. Next, the privacy-as-secrecy conceptualization was discussed. As citizens have become compelled to surrender personal data in order to function in society, the privacy-as-secrecy conceptualization has been weakened by the necessity of recognizing limited privacy wherein individuals can retain some privacy in information they have shared with third-parties. Lastly, the privacy-as-information-control conceptualization was discussed. Central to this conceptualization and its variants, privacy-as-property or privacy-as-contract, is personal agency. When the right to privacy is conceived of this way, privacy law functions to empower individuals to control access to their personal information.

The common element among all of these conceptualizations and their variants is the control of information flow. None has succeeded in defining privacy or the value of privacy in every context, but they all ultimately describe an individual's ability to conceal, manipulate, or share personal information. These conceptualizations are used in the chapters that follow as a framework in which to analyze what the U.S. Supreme Court and the U.S. Circuit Courts of Appeal have said about the fundamental right to control personal information in First and Fourth Amendment jurisprudence and within the emerging information privacy doctrine.

Research Questions

This dissertation addresses the following research questions:

RQ1: How has the U.S. Supreme Court conceptualized the constitutional right to privacy in general in First and Fourth Amendment privacy jurisprudence?

*RQ2***:** How have the U.S. Supreme Court and U.S. Circuit Courts of Appeal conceptualized the constitutional right to information privacy?

RQ3: What are the strengths and weaknesses of the current conceptualizations of the constitutional right of privacy in general or the constitutional right of information privacy in particular as protection against KDD?

RQ4: If a conceptualization more protective of information privacy is needed, what should it be? How might KDD applications and policies be designed to better comply with the individual constitutional right to avoid the disclosure of personal matters?

Method

This dissertation presents a traditional legal case analysis involving three types of case law. First, U.S. Supreme Court First Amendment anonymous speech and association cases and Fourth Amendment privacy cases are examined in turn. Then Supreme Court and U.S. Circuit Courts of Appeal cases thatdiscuss information privacy as either a protected liberty under the Due Process Clause of the Fourteenth Amendment[154] or as an implied right under one of the Amendments in the Bill of Rights[155] are analyzed. Language from each decision is examined in order to identify the conceptualization(s) of privacy implicit or explicit in the court's determination of the privacy interest at risk in each case: privacy as space, privacy as secrecy, or privacy as information control. Evidence is also sought regarding the emergence of any new conceptualizations of privacy not discussed in privacy scholarship reviewed above.

Within each of the three types of case law, analysis is conducted chronologically in order to identify the historical evolutionary progression of the courts' conceptualizations of privacy within each doctrine. Conceptual trends revealed in the First Amendment, Fourth Amendment, and information privacy law are discussed in terms of which conceptualization is most likely to underlie the courts' decisions in any future constitutional challenge to the use of KDD technologies.

A preliminary list of 135 cases was generated using three methods. First, Westlaw database searches were conducted using combinations of the following search terms:

---

[154] U.S. CONST. amend, XIV, § 1. The clause reads: "[N]or shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws." These cases typically involve a constitutional challenge to a federal, state, or local statute which compels individuals to surrender personal information.

[155] *See* Griswold v. Connecticut, 318 U.S 479, 484 (1965).

First Amendment, freedom of speech, privacy, surveillance, dataveillance, information privacy, database(s), Fourth Amendment, and Fourteenth Amendment. Second, following a cursory review, decisional and statutory privacy cases were removed and the preliminary case list was divided into two categories: First Amendment anonymous speech and association cases and Fourth Amendment privacy cases. The landmark cases were then selected from these shorter lists. The landmark cases are those most often cited by the Supreme Court in its privacy jurisprudence and are the most referenced in the scholarly literature. This resulted in a list of ten First Amendment cases and twelve Fourth Amendment cases that are analyzed in chapters 2 and 3 respectively.

Information privacy is a new and vaguely defined legal doctrine that began with the Supreme Court's decision in *Whalen v. Roe.*[156] The Supreme Court has only decided one case, *Nixon v. Administrator of General Services*,[157] since *Whalen* that has further shaped the Court's information privacy doctrine. Therefore, a list of U.S. Circuit Courts of Appeal information privacy cases was generated by using LexisNexis to *Shepardize* the phrase "interest in avoiding the disclosure of personal matters" from *Whalen*. The process yielded a list of 264 cases. All district court cases and circuit court decisions that merely cited to the language in *Whalen* were eliminated, and a core of twenty appellate decisions in which the phrase was followed, explained, distinguished, or criticized remained. These twenty cases are analyzed in Chapter 4.

Chapter 5 details the KDD process, which has two distinct stages: pre-KDD processes and KDD applications, and applies the five privacy conceptualizations to the

[156] 429 U.S. 589 (1977).

[157] 433 U.S. 425 (1977).

second stage. Chapter 6 summarizes the answers to the four research questions presented above.

Study Limitations

This study is an exploration of the conceptualizations of a constitutional right to privacy in general and information privacy in particular. It discusses how these rights have been articulated by the Supreme Court and the U.S. Courts of Appeal and also how they might be applied to the use of KDD by the federal government. There are a number of related areas that this dissertation does not address. It does not delve into issues of criminal law that are related to information privacy. Issues arising under the Fifth and Sixth Amendments regarding self-incrimination and fair trial are not discussed. Neither are evidentiary rules that might affect the admissibility of evidence gathered through the use of dataveillance discussed. No statutory privacy protections or privacy torts are discussed, and no case law arising from privacy rights granted in state constitutions is discussed. Also, other than the circuit court opinions discussed in Chapter 4, cases from the lower federal courts and state courts are beyond the scope of this dissertation, as are the many policy debates about dataveillance.

CHAPTER II

THE FIRST AMENDMENT: PRIVACY AND ANONYMITY

Privacy within First Amendment jurisprudence has been conceptualized as the right to control the dissemination of personal information, especially one's identity, and to a lesser extent, as a right to limit access to one's self. It has been used by the Supreme Court to defend both anonymous speech and anonymous association. Since First Amendment privacy cases involve challenges to the government's ability to directly compel individuals to surrender identifying information, comprehension of how privacy has been conceptualized in First Amendment privacy jurisprudence will be useful for evaluating current privacy protections against the government's use of KDD dataveillance.

Though the word "anonymous" does not appear in the First Amendment,[158] through the application of historical analysis, the Court has recognized that anonymous speech was highly valued by the Framers as a tool for protecting those expressing

[158] Talley v. California, 362 U.S. 60, 70 (1960) (Clark, J., dissenting). "The Constitution says nothing about freedom of anonymous speech. In fact, this Court has approved laws requiring no less than Los Angeles' ordinance." Justice Clark is referring to *Lewis Pub. Co. v. Morgan*, 229 U.S. 288 (1913), which upheld an Act of Congress (39 U.S.C. § 233) requiring any newspaper using the second-class mails to publish the names of its editor, publisher, owner, and stockholders and *United States v. Harris*, 347 U.S. 612 (1954), which upheld The Federal Regulation of Lobbying Act, (2 U.S.C. § 267) requiring those engaged in lobbying to divulge their identities and give 'a modicum of information' to Congress.

political views.[159] Moreover, in *NAACP v. Alabama* [160] the Court recognized "the vital relationship between freedom to associate and privacy in one's associations."[161]

This chapter discusses five Supreme Court anonymous speech cases decided between 1943 and 2002 and five Supreme Court anonymous association cases decided between 1958 and 1972. These ten cases were identified as landmark cases in the scholarly literature and were frequently cited in subsequent First Amendment privacy cases. Beginning in the mid-twentieth century, events such as the Civil Rights movement, McCarthyism, and the peace movement during the Vietnam conflict rekindled the government's desire, at all levels, to identify individuals who held dissident viewpoints. The cases discussed below resulted from challenges to state action in this regard. This chapter reveals that throughout these First Amendment privacy cases the Court has primarily conceptualized the constitutional right to privacy as one of information control.

In cases involving First Amendment anonymity, the Court must decide whether, in a particular circumstance, the government is empowered to compel the disclosure of identifying information. Therefore, anonymity is necessarilypredicated upon information control. Nevertheless, the acceptance of privacy-as-access-to-self variant of

---

[159] McEntyre v. Ohio Elections Comm'n, 514 U.S. 334, 343, n.6 (1995). In the Court's dicta. examples are provided of politicians in history who opted to write anonymously under pseudonyms. The list includes: Publius (James Madison, Alexander Hamilton, and John Jay), Cato (allegedly New York Governor George Clinton), Centinel (probably Samuel Bryan or his father, George Bryan), The Federal Farmer (maybe Richard Henry Lee), Brutus (likely Robert Yates), and Junius (a pre-revolutionary English pamphleteer as yet unidentified); *see also id*. at 360-71 (Thomas, J., concurring). Justice Thomas provided a thorough, historical argument to support his assertion that given the historical context in which the First Amendment was drafted, the Founders intended the First Amendment to protect the individual's right to express thoughts and opinions regarding political candidates or issues in an anonymous manner.

[160] 357 U.S. 449 (1958).

[161] *Id*. at 465.

the privacy-as-space conceptualization is subsumed within the Court's recognition of a right to control identifying information. Justice William O. Douglas once wrote, " [T]he right of privacy implicit in the First Amendment creates an area into which the Government may not enter."[162] This "area" is the inviolate personality discussed by Warren and Brandeis.[163] It is the interior realm in which individuals guard their most intimate beliefs, knowledge, and values. Constitutional privacy protections under the First Amendment protect individuals from being compelled by the government to surrender this type of personal information.

For purposes of this analysis, the term "anonymous speech" is used in reference to any instance when an individual chooses to speak, publish, or distribute information without revealing his or her identity. Among other functions, anonymous speech has been considered to reduce the chance of retribution for the expression of unpopular sentiment,[164] to remove listeners' perceptions of a speaker from the process of evaluating the merit of the information being disseminated,[165] to allow those seeking information on sensitive topics to feel less apprehension, and to allow for the preservation of as much privacy as possible.[166]

---

[162] Gibson v. Florida Legis. Investigation Comm., 372 U.S. 539, 569-70 (1963) (Douglas, J., concurring).

[163] Warren & Brandeis, *supra* note 48, at 205.

[164] *McEntyre*, 514 U.S. at 341-42 "The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible."

[165] *Id*. at 342. "[A]n advocate may believe her ideas will be more persuasive if her readers are unaware of her identity. Anonymity thereby provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent."

[166] *See generally* MADELEINE SCHACHTER, LAW OF INTERNET SPEECH, 311-14 (2d. ed. 2002) (describing in broad terms the social values served by anonymous speech).

The term "anonymous assembly" or "anonymous association" is used to describe an instance in which individuals would prefer not to share with the government a list of groups to which they belong, of those they support, or of fellow members. Like anonymous speech, anonymous association plays a vital role in self government. In *NAACP*, the Court recognized that the "inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."[167] Framed in this manner, anonymity promotes individual and group sovereignty through the exercise of the right to control the disclosure of identifying information.

Privacy in Anonymous Speech Cases

In anonymous speech cases involving the distribution of pamphlets, the collection of signatures on petitions, and door-to-door proselytizing, the Court has recognized that individuals have a right to limit access to their selves by controlling the disclosure of their identity to others. The individual privacy interest is the ability to avoid any retaliatory harms that might result when those receiving unpopular or offensive information are able to identity those disseminating it. In none of the anonymous speech cases reviewed did the government put forth a substantial reason for compelling the disclosure of such personal information. In adopting the privacy-as-information-control conceptualization, the Court concomitantly recognized limited privacy. Individuals do not automatically surrender the right of anonymity because they disclose, by standing

[167] NAACP v. Alabama, 357 U.S. 449, 462 (1958).

physically in front of others distributing leaflets, that they support a specific belief, cause, or candidate. Other bits of personal information can still be concealed.

An iconic construct in First Amendment jurisprudence has been the "Lonely Pamphleteer,"[168] a mythic champion for those who espouse unpopular views in the marketplace of ideas despite what John Stuart Mill would have called the tyranny of the majority.[169] During the twentieth century the Court has ruled on cases involving pamphleteers who allegedly threatened national security by disseminating subversive materials,[170] who violated city ordinances designed to prevent littering,[171] who violated ordinances designed to protect homeowners from those distributing literature door-to-door,[172] and who violated ordinances designed to prevent fraud in elections.[173]

---

[168] *See* Branzburg v. Hayes, 408 U.S. 665, 703 (1972) (lamenting the difficulty of determining whether the "liberty of the press is the right of the lonely pamphleteer who uses carbon paper or a mimeograph just as much as [it is a right] of the large metropolitan publisher who utilizes the latest photocomposition methods").

[169] *See*, *e.g.*, John Stuart Mill, *On the Liberty of Thought and Discussion*, ON LIBERTY, ch. 2 (1869), *available at* http://www.utilitarianism.com/ol/two/html. Mill argued that protection against the state is not enough; individual expression also needs to be protected against the tyranny of the prevailing opinion and feeling in society; against the tendency for society to impose its owns ideas, practices, and rules of behavior on those who dissent from them. Social stigma is a powerful tool of repression when used against dissenters.

[170] *See* Schenck v. United States, 249 U.S. 47 (1919) (holding that distributing circulars to men about to be drafted that encouraged insubordination and draft resistance was a violation of the Espionage Act of 1917), Abrams v. United States, 250 US 616 (1919) (convicting five Russian Jews of violating the Espionage Act of 1917 for distributing two anarchist circulars (entitled *The Hypocrisy of the United States and her Allies* and *Workers Wake Up* respectively) including "some by throwing them from a window of a building where one of the defendants was employed in New York City"), *and* Gitlow v. United States, 268 U.S. 652 (1925) (convicting Gitlow, a socialist during the nation's first "Red Scare," of criminal anarchy for violating a New York City ordinance when he "printed, published and knowingly circulated and distributed a certain paper called 'The Revolutionary Age,' containing the writings . . . advocating, advising and teaching the doctrine that organized government should be overthrown by force, violence and unlawful means").

[171] *See* Schneider v. State, 308 U.S. 147 (1939).The primary rationales behind both § 28.01 of the Los Angeles Municipal Code and Milwaukee ordinance St.1937, § 103.53(1)(e) were to prevent littering, which was perceived as an undesirable byproduct of distributing handbills. Both ordinances were struck down as unconstitutional restrictions upon free speech.

[172] These were primarily nuisance laws aimed at eliminating the annoyance caused by door-to-door canvassing or solicitation.

Most of these cases resulted in the Court ruling that city ordinances prohibiting the distribution of handbills, pamphlets, or leaflets on city streets or door-to-door were generally unconstitutional restrictions of free speech.[174] These decisions stressed the central role this method of sharing information has played in the history of the United States. As Chief Justice Charles Evans Hughes wrote in *Lovell v. City of Griffin* that pamphlets and leaflets "indeed have been historic weapons in the defense of liberty, as the pamphlets of Thomas Paine and others in our own history abundantly attest."[175]

Once such outright prohibitions on distributing pamphlets, handbills, etc. were ruled unconstitutional, cities began to "condition" their distribution. A number of city ordinances did so by requiring those disseminating information to obtain permits from the city. The permit application process necessarily forced individuals to surrender their identifying information to the government in order to participate in public discourse.[176] Justice Hugo Black stressed the importance of the anonymity threatened by such

---

[173] McEntyre v. Ohio Elections Commission, 514 U.S. 334 (1995). The Court struck down § 3599.09(A) of the Ohio Code, which prohibited the distribution of "campaign literature that does not contain the name and address of the person or campaign official issuing the literature."

[174] Many cities passed nuisance laws designed to stop canvassers, religious missionaries, salespersons, petitioners, etc. from either passing out literature in public areas, preaching/speaking on street corners, etc., or from going door-to-door. A number of these statutes and ordinances were challenged by Jehovah's Witnesses who felt they were commanded by Jehovah to spread his truth, and thus any man-made law was considered an insult to their religious practice.

[175] Lovell v. City of Griffin, 303 U.S. 444, 451-52 (1938). In this case the Court ruled that a city ordinance that prohibited "the distribution of literature of any kind at any time, at any place, and in any manner without a permit from the city manager" would in fact "restore the system of license and censorship in its baldest form" and thus was unconstitutional.

[176] *See Schneider*, 308 U.S. at 157-58. The Court overturned an Irvington, New Jersey, ordinance that required that each "canvasser must make an application giving his name, address, age, height, weight, place of birth, whether or not one was previously arrested or convicted of crime, by whom employed, address of employer, clothing worn, and description of project for which he is canvassing; [and] that each applicant shall be fingerprinted and photographed."

ordinances in the 1960 case *Talley v. State of California.*[177] Justice Black wrote: "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all."[178]

Since anonymity had already been recognized as a vital element in political speech, the Court was tasked with balancing the legislative purpose for prohibiting anonymity against the individual's right to keep identifying information private. Thus, the "pamphleteer" cases yield a rich vein of anonymous speech jurisprudence, which provides insight into the Court's conceptualization of privacy in First Amendment free speech doctrine.

Anonymity and Pamphleteering

Talley was the first "pamphleteer" case in which the Supreme Court ruled on the right to anonymity for those distributing handbills. The Court recognized anonymity as the individual right to control the disclosure of identifying information for the purpose of limiting access to one's self, to keep one's inner realm private. The Court thus subsumed the privacy-as-access-to-self conceptualization of privacy under the privacy-as-information-control conceptualization. Understood in this way, one's right to protect the

[177] 362 U.S. 60 (1960).

[178] *Id*. at 64. He went on to argue that the English seditious libel cases of John Lilburne, John Penry, and John Udal demonstrate the lengths to which governments would go to silence opposition.

self is only actualized through the exercise of the broader right to control access to personal information.

At issue in *Talley*was a challenge to a Los Angeles, California, ordinance that required that the name and address of the person(s) or group(s) responsible for producing and distributing any handbills, leaflets, etc. be printed on all literature disseminated within the city.[179] The question before the Court was whether government can burden individuals desiring to participate in public discourse with the compelled disclosure of personally identifying information.

Justice Black drew on American history to establish that anonymity had often been "assumed for the most constructive purposes."[180] He compared the individual handing out handbills in Los Angeles to the Founding Fathers when he focused on the harms that might befall those speaking publicly. For instance, he wrote, "Before the Revolutionary War colonial patriots frequently had to conceal their authorship or distribution of literature that easily could have brought down on them prosecutions by English-controlled courts."[181] He then noted that the justification of preventing such harms had also been used by the Court in mid-twentieth century anonymous assembly cases wherein statutes that compelled the disclosure of group membership lists were

[179] L.A., CAL. MUNICIPAL CODE § 28.06. This section provided that "no person shall distribute any hand-bill in any place under any circumstances, which does not have printed on the cover, or the face thereof, the name and address of the following: (a) The person who printed, wrote, compiled or manufactured the same. (b) The person who caused the same to be distributed; provided, however, that in the case of a fictitious person or club, in addition to such fictitious name, the true names and addresses of the owners, managers or agents of the person sponsoring said hand-bill shall also appear thereon." The handbill at question in *Talley* urged citizens to boycott certain businesses with allegedly discriminatory hiring practices and was labeled as being from the National Consumers Mobilization.

[180] *Talley*, 362 U.S. at 64-65.

[181] *Id*. Justice Black used the Letters of Junius and the Federalist Papers as examples of these revolutionary era writings.

struck down because "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance."[182] The Court in *Talley* ruled that the Los Angeles ordinance was "subject to the same infirmity" and thus, likethe ordinance in *Lovell*, was "unconstitutional on its face." [183]

In *Talley* the Court implicitly recognized the privacy-as-information-control conceptualization. The decision empowered individuals to control access to their identities, and in doing so it legitimized the notion of limited privacy. For instance, it could be argued that in choosing to stand in a public place and distribute literature, individuals are surrendering their right to personal privacy. As discussed in chapter one, under the privacy-as-secrecy paradigm, any information shared with a third party cannot be private, and, had the Court utilized that conceptualization it could have ruled that one shares one's entire identity when standing bodily in front of others. Reasoning under the privacy-as-secrecy conceptualization incorporates an all-or-nothing concept of personal information.

Instead, in striking down the ordinance because an "identification requirement would tend to restrict freedom to distribute information and thereby freedom of expression,"[184] the *Talley*Court recognized that individuals can choose to identify themselves with a belief or political stance without providing any other information about themselves. Justice Black empowered individuals to share select aspects of their identity without surrendering complete access to themselves to the government and, by extension, to those to whom they distribute literature.

---

[182] *Id.* at 65.

[183] *Id.*

[184] *Id.* at 64.

Ultimately, the *Talley* decision is about the Court allocating the power to control information. This ruling is also important because not all personal information is created equal. To know an individual's name is to gain the ability to access additional personal information about that person. For example, if a person's name is known, it is rather simple to access his or her phone number, but it is slightly more difficult to access his or her name given a phone number. Certain bits of information, like an address or a Social Security number, provide a "gateway" through which one might learn more about another person. The permit requirement in *Talley* involved such "gateway" information. By striking down the Los Angeles ordinance, the Court recognized privacy as the individual right to control personal information in general and thereby to limit access to one's self as well as to enjoy limited privacy in contrast to the commoditized, all-or-nothing, privacy-as-secrecy conceptualization.

Privacy as information control was also evident in the next landmark ruling involving anonymous speech and the distribution of handbills, *McEntyre v. Ohio Elections Commission.*[185] Whereas the handbill in *Talley* called for an economic boycott, the literature in *McEntyre* was part of the political process itself in that it encouraged voters to vote down a proposed school tax. Justice John Paul Stevens referenced the Court's reasoning in *Talley,* which he thought supported "a respected tradition of anonymity in the advocacy of political causes . . . perhaps best exemplified by the secret ballot, the hard-won right to vote one's conscience without fear of retaliation."[186] Justice Stevens framed the question in *McEntyre* as "whether and to what extent the First

[185] McEntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995). Ohio's statute prohibiting the distribution of any anonymous campaign literature was held unconstitutional.

[186] *Id.* at 343.

Amendment's protection of anonymity encompasses documents intended to influence the electoral process."[187]

The Ohio statute under scrutiny in *McEntyre* prohibited the distribution of any campaign literature that did not include, on its face, "the name and residence or business address of the chairman, treasurer, or secretary of the organization issuing the same, or the person who issues, makes, or is responsible therefore."[188] The Court ruled that the statute was a regulation of "pure speech" as it did not directly control "the mechanics of the electoral process,"[189] and, therefore, the Court needed to apply "exacting scrutiny."[190] Similar to Justice Black in *Talley*, Justice Clarence Thomas, in his *McEntyre* concurrence, stressed the importance of anonymity in the American tradition.[191] He wrote:

> Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. . . . Anonymity is a shield from the tyranny of the majority . . . . It thus exemplifies the purpose behind the Bill ofRights and of the First Amendment in particular: to protect unpopular individuals from retaliation -- and their ideas from suppression -- at the hand of an intolerant society.[192]

---

[187] *Id.* at 344.

[188] OHIO REV.CODE ANN. § 3599.09(A) (1988).

[189] *McEntyre*, 514 U.S. at 345.

[190] *Id.* at 347.

[191] *Id.* at 370 (Thomas, J., concurring). Justice Clarence Thomas, following a lengthy and detailed historical analysis of anonymous authorship in American political history, concluded, "After reviewing the weight of the historical evidence, it seems that the Framers understood the First Amendment to protect an author's right to express his thoughts on political candidates or issues in an anonymous fashion."

[192] *Id.* at 357.

The disclosure statute was ruled unconstitutional because Ohio's stated interests in "providing voters with additional relevant information" and in preventing the likelihood of election fraud did not justify a "state requirement that a writer make statements or disclosures she would otherwise omit."[193]

Like Justice Black had in *Talley*Justice Stevens recognized that disclosing personal information to the government placed individuals at risk for nothing more than exercising their fundamental right to free speech. He recognized the right of individuals to decide when and to whom to make information about themselves accessible, the privacy-as-information-control conceptualization. In *McEntyre*, Justice Stevens explicitly described the importance of this ability to control identifying information as the ability to protect the self. He used language reminiscent of Warren and Brandeis' notion of "inviolate personality."[194] He wrote: "A written election-related document -- particularly a leaflet – is often a personally crafted statement of a political viewpoint. . . . As such, identification of the author against her will is particularly intrusive; it reveals unmistakably the content of her thoughts on a controversial issue."[195]

Since the purpose of a political handbill is ultimately to persuade, it stands to reason that an individual's reasons for supporting a particular position or candidate would be printed on the handbill. These talking points may directly expose the pamphleteer's deeply held beliefs and values and thus provide a window into one's personality. Justice

[193] *Id.* at 348-49.

[194] Warren & Brandeis, *supra* note 48, at 205.

[195] *McEntyre*, 514 U.S. at 355.

Stevens reasoned that a compelled disclosure of one's identity, in combination with such a statement of belief, exposed too much of the self.

As it was in *Talley*, limited privacy was central to the *McEntyre* Court's reasoning. Justice Stevens explicitly recognized that political literature often exposes what an individual thinks, believes, or supports, but without "gateway" knowledge, the pamphleteer is able to remain anonymous. Absent "identifying" information individuals are better shielded from the possibility of private retaliation enabled by government mandated disclosure.

Four years after *McEntyre*, the Courtagain conceptualized privacy as limiting access-to-self through the exercise of a right to control identifying information as it considered the value of anonymity to individuals collecting signatures on petitions in public places. Justice Ruth Bader Ginsburg wrote for the majority in *Buckley v. American Constitutional Law Foundation*,[196] wherein the Court struck down as unconstitutional restrictions of free speech provisions in a Colorado statute that required initiative-petition circulators[197] to wear identification badges[198] and proponents of a ballot initiative to report the names, addresses, and salaries of all paid circulators.[199] Also weighed in the Court's analysis was that initiative proponents were required to submit an affidavit (at the time they file their petition) containing the name, address, and county of

[196] Buckley v. Am. Const. Law Found., 525 U.S. 182 (1999).

[197] Colorado allows citizens to make laws directly by placing ballot issue initiatives in elections once enough signatures are obtained on initiative petitions. This case involved constitutional challenges to six rules intended to control the ballot-initiative process.

[198] COL. REV. STAT. § 1-40-112(2). Along with the circulator's name, his or her status as "paid" or "volunteer" had to be noted. Badges on circulators who were paid also had to note who was paying them.

[199] COL. REV. STAT. § 1-40-121. This information was to be submitted as part of an affidavit submitted with completed petitions.

voter registration of all paid circulators; the amount of money proponents paid per petition signature; the total amount paid to each circulator; and reports ofmonthly totals containing the names of the proponents, the name and address of each paid circulator, the name of the proposed ballot measure, and the amount of money paid and owed to each circulator each month.[200]

Central to Justice Ginsburg's reasoning was the potential harm to individuals circulating the initiative-petitions. Again, the issue was that individuals should have the ability to control the revelation of personal information to others, especially in situations where there was a heightened possibility of retaliatory harm. Justice Ginsburg distinguished between the levels of risk associated with the affidavit disclosures and the name badge requirements. She wrote: "While the affidavit reveals the name of the petition circulator and is a public record, it is tuned to the speaker's interest as well as the state's. Unlike a name badge worn at the time a circulator is soliciting signatures, the affidavit is separated from the moment the circulator speaks."[201]

In *Talley* and *McEntyre* the Court had recognized that individuals have a right to limited privacy regarding their identity when handing someone a pamphlet. In *Buckley* the Court ruled that the decision to disclose one's identity lies with the individual who, at the moment of face-to-face communication, can best assess the level of risk of retaliation by those receiving their information. This notion was intimated when Ginsburg wrote, "The injury to speech is heightened for the petition circulator because the badge

---

[200] *Id.*

[201] *Buckley*, 525 U.S. at 198-99. Should anyone receiving the information in question become passionate, offended, or enraged, they might note the petitioner's name and plan some type of future retribution. Should a name or identifier not be visible, the recipient's emotional response might ebb before he or she is able to attain the petitioner's identity.

requirement compels personal name identification at the precise moment when the circulator's interest in anonymity is greatest."[202] Thus, again, the Court's conceptualization of privacy was as a right to limit access to self through a right to control access to personal information, and this privacy interest is increasingly heightened as the immediate threat of harm increases.

In regard to the personal information that Colorado required to be submitted on the affidavit when petitions are turned in, the Court recognized a lesser privacy interest. Relying on language from the Tenth Circuit decision,[203] Ginsburg noted, "The affidavit, in contrast, does not expose the circulator to the risk of 'heat of the moment' harassment"[204] because the affidavits, though public records, are not instantly accessible and less likely to be used to harm the initiative-petition circulators in some way. This is a concept running throughout First Amendment anonymous speech and association cases; the more remote the risk of potential harm, the exact nature of which was never defined by the Court, the lesser the individual privacy interest relative to the state.

Thus, in *Buckley,* Colorado's name badge requirement was struck down and the affidavit disclosure provision was allowed to stand. Underlying this distinction is the concept of "practical obscurity," which is a term used in reference to how difficult information is to access.[205] The Court first recognized this concept in 1989 in *U.S. Dept.*

---

[202] *Id.* at 199-200.

[203] Am. Const. Law Found. v. Meyer, 120 F.3d, 1092, 1102 (10th Cir. 1997).

[204] *Buckley*, 525 U.S. at 198-99.

[205] *See* SYKES, *supra* note 22, at 254 (explaining that "one of the elements of privacy enjoyed in the past was precisely the 'practical obscurity' of personal information. The Court not only found that individuals had a genuine privacy interest in keeping their criminal past out of the public domain, but they also had an interest in the 'practical obscurity' of a precomputerized age.").

of Justice v. Reporters Committee for Freedom of Press.[206] In this case a descendant of a suspected mob criminal filed an injunction to prevent disclosure to the press of his father's criminal record. Individual "rap sheets" had recently been compiled into a centralized government database. Prior to this compilation, such information, though public records, had been scattered throughout a number of states and government departments. It was a laborious task to compile someone's complete rap sheet. The impracticality of doing so actually served as a layer of privacy protection for personal information.[207] This layer ofprotection dissolved when records were combined in accessible databases.

Justice Ginsburg used similar reasoning to Justice Stevens' in *Reporters Committee.* Those canvassing for signatures on initiative petitions could be too easily identified by name badges just as Charles Medico's criminal records were too easily obtainable in a computerized database. Without the name badge requirement, practical obscurity could balance the interests of the speaker and the city. It would require an investment of time for someone who had been annoyed by a petition circulator to go to the Board of Elections and request a copy of the initiative proponent's filed affidavit, then to learn the name and address of the petition circulator, and then plan some retaliatory action.

---

[206] 489 U.S. 749 (1989). Records for Charles Medico were requested by the media under the federal Freedom of Information Act (FOIA), 5 U.S.C. § 552(a)(1)(C) (2002). The U.S. Supreme Court ruled that disclosure of these compiled files was an unwarranted invasion of privacy and thus qualified for a FOIA exemption under § 552(b)(7)(C).

[207] *Id.* at 764. Justice John Paul Stevens wrote: "[T]he issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."

The Colorado provisions at issue in *Buckley* allegedly allocated too much power to the state. This threat to personal privacy was closely related to one of the core values of the U.S. Constitution, limited government, because the rules under review directly governed elections. Should individuals be chilled from participating in the democratic process, then these provisions would have directly impeded the power of the people to self-govern. The Court recognized that the provisions destroyed "practical obscurity" and the ability of individuals to control access to identifying information, and was able to restore the balance in the relationship between voters and the state by striking down the name badge provision and upholding the affidavit disclosures.

Anonymity and Canvassing

In the preceding pamphleteering cases the Court upheld the individual privacy interest in avoiding any potential retaliatory harms that might result from the disclosure of one's identity against various city and state interests in preventing littering, informing voters, and preventing fraud. In each case pamphlets were being distributed in a public space, but the Court has also evaluated anonymity, and thus privacy, in instances where individuals desired to distribute literature or collect signatures going door-to-door in neighborhoods thathad ordinances in place to prohibit such behavior .

In these canvassing cases the Court balanced two separate individual privacy interests: that of the homeowners who did not want to be disturbed and that of canvassers who did not want to be compelled to disclose their identities in exchange for permission to canvass neighborhoods. Both of these interests were conceptualized as the right to control the flow of information. Canvassers, like the pamphleteers in the preceding

cases, had an interest in controlling the disclosure of their identity. Homeowners had an interest in being able to control the flow of general information into their homes.

Just as some cities and states had attempted to enact outright bans on the distribution of pamphlets in public spaces, in some cases similar bans were passed regarding door-to-door canvassing. In 1943 the Court struck down as "the naked restriction of the dissemination of ideas"[208] a city ordinance that completely banned door-to-door distribution of literature whether for "political, social, religious, or commercial purposes."[209] In *Martin v. City of Struthers,*[210] Justice Black wrote for the majority and embraced the every-man's-house-is-his-castle philosophy. He used language that signaled his belief that the spatial privacy conceptualization was all about the right of homeowners to control the flow of information into their homes. In the opening lines of the *Martin* decision, Justice Black wrote:

> For centuries it has been a common practice in this and other countries for persons not specifically invited to go from home to home and knock on doors or ring doorbells to communicate ideas to the occupants or to invite them to political, religious, or other kinds of public meetings. Whether such visiting shall be permitted has in general been deemed to depend upon the will of the individual master of each household, and not upon the determination of the community.[211]

[208] Martin v. City of Struthers, 319 U.S. 141, 147 (1943).

[209] *Id.* The city ordinance read as follows: "It is unlawful for any person distributing handbills, circulars or other advertisements to ring the door bell, sound the door knocker, or otherwise summon the inmate or inmates of any residence to the door for the purpose of receiving such handbills, circulars or other advertisements they or any person with them may be distributing."

[210] 319 U.S. 141 (1943).

[211] *Id.* at 141.

Implied here is that individuals have a First Amendment right to share information door-to-door, but private property rights are more important than the First Amendment rights in this context.[212]

The *Martin* decision did reinforce a private property right, but Justice Black seemed to conceive of this right as one of information control. He reasoned that homeowner privacy was preserved when the law provided mechanisms through which residents could limit the flow of outside information into their private space. This sentiment was also noted in a concurrence by Justice Felix Frankfurter who wrote, "Door-knocking and bell-ringing by professed peddlers of things or ideas may . . . be confined within specified hours and otherwise circumscribed so as not to sanctify the rights of these peddlers in disregard of the rights of those within doors."[213]

Justice Black provided a summary of state trespass laws and noted, "Traditionally the American law punishes persons who enter onto the property of another after having been warned by the owner to keep off."[214] Thus, Justice Black established that homeowners' privacy was protected by state trespass law and that time, place, and manner restrictions on canvassing would be constitutional. He asserted that any dangers associated with the distribution of literature were easily controlled by "traditional legal methods" that left to each homeowner "the full right to decide whether he will receive strangers as visitors."[215] This right of homeowners to decide whether to receive visitors

---

[212] *Id.* at 146-47. Justice Black wrote, "Freedom to distribute information to every citizen wherever he desires to receive it is so clearly vital to the preservation of a free society that, putting aside reasonable police and health regulations of time and manner of distribution, it must be fully preserved."

[213] *Id.* at 153. (Frankfurter, J., concurring).

[214] *Id*. at 147.

[215] *Id.*

should be understood as a right to control the flow of information into their homes.

The privacy rights of both homeowners and canvassers were again balanced in *Watchtower Bible & Tract Society of New York v. Village of Stratton.*[216] Here, the Court had to balance the privacy interest of the homeowners, which was conceptualized in much the same way as it had been in *Martin*, against the right of individuals to control the disclosure of their identifying information.

In *Watchtower* the Court reviewed a First Amendment challenge to a Stratton, Ohio, ordinance that prohibited "canvassers and others" from going on private residential property to promote any cause without first obtaining a "solicitation permit" thatwas to be carried by individuals going door-to-door and shown to any home resident upon request.[217] Canvassers were required to fill out a lengthy permit application (which asked for one's name, home address, purpose, employer, and residence(s) for the previous five years among other bits of information), which would be kept on file with the mayor's office in Stratton.

The Sixth Circuit had previously upheld the Stratton ordinance.[218] Rejecting the idea of limited privacy, the appellate court held:

> [I]ndividuals going door-to-door to engage in political speech are not anonymous by virtue of the fact that they reveal a portion of their identities -- their physical identities -- to the residents they canvass, . . . [T]he very act of going door-to-door requires the canvassers to reveal a portion of their identities.[219]

---

[216] 536 U.S. 150 (2002).

[217] ORD. NO. 1998-, §§ 116.01-03.

[218] Watchtower Bible & Tract Soc'y of N.Y. v. Vill. of Stratton , 240 F.3d 553 (6th Cir. 2001).

[219] *Id.* at 563.

The circuit court then reasoned that the ordinance did not force individuals to surrender their entire identities, only "the remainder of their identities, i.e., their names."[220]

Justice John Paul Stevens wrote the U.S. Supreme Court opinion in *Watchtower* and framed the legal issue this way: "Does a municipal ordinance that requires one to obtain a permit prior to engaging in the door-to-door advocacy of a political cause and to display upon demand the permit, which contains one's name, violate the First Amendment protection accorded to anonymous pamphleteering or discourse?"[221] The Court said the village ordinance applied not only to the "religious proselytizing" that had triggered the case, "but also to anonymous political speech and the distribution of handbills."[222] The Court overturned the Sixth Circuit decision and struck down the ordinance as an unconstitutional restriction of free speech.

Whereas the lower court applied the all-or-nothing model of surrendering one's personal information more common under the privacy-as-secrecy conceptualization, the Supreme Court again accepted the idea of limited privacy as it had in *Talley, McEntyre*, and *Buckley.* Justice Stevens wrote, "[In *Buckley*], the fact that circulators revealed their physical identities did not foreclose our consideration of the circulators' interest in maintaining their anonymity."[223] Stevens noted that strangers to the residents of Stratton maintained their anonymity even in door-to-door canvassing and that "the ordinance may preclude such persons from canvassing for unpopular causes."[224]

---

[220] *Id*.

[221] *Watchtower*, 536 U.S. at 160.

[222] *Id.* at 153.

[223] *Id.* at 167.

[224] *Id.*

Justice Stevens left the door open for future regulation of door-to-door canvassing by noting that such an ordinance may be justified in "some situations" such as "protecting the integrity of a ballot-initiative process" or "the interest in preventing fraudulent commercial transactions."[225] However, the Court considered the village ordinance to be overly broad because it "[covered] unpopular causes unrelated to commercial transactions or to any special interest in protecting the electoral process."[226] Thus again in *Watchtower* the Court recognized that a right of anonymity, predicated on the notion of limited privacy, exists under the First Amendment. Individuals rather than the state control access to themselves by exercising a right to control identifying information.

The Court in *Watchtower* also explicitly recognized the privacy-as-space conceptualization in its discussion of Stratton residents' ability to limit solicitations. Similar to *Martin*, it did so by discussing how the law enabled homeowners to control the information flow into their homes. Homeowners in Stratton were able to file a "No Solicitation Registration Form" with the mayor's office.[227] The form was designed to allow homeowners to either prohibit all home solicitations or to prohibit members of certain groups from entering their property.

Even if canvassers had filed for and received a "solicitation permit," they were required to abide by the list of homeowners who had filed no-solicitation registration forms. These solicitation bans were legally enforceable by property holders who had both filed the no-solicitation form and posted a "No Solicitation" sign on their property.

---

[225] *Id.*

[226] *Id.*

[227] ORD. NO. 1998, § 107.

One of the justifications put forth by Stratton for the ordinance was to protect the privacy of homeowners. The Court reasoned that since "the annoyance caused by an uninvited knock on the front door is the same whether or not the visitor is armed with a permit,"[228] disclosure of one's identity was not relevant to the purpose of the ordinance. Justice Stevens wrote, "With respect to [protecting homeowner privacy], it seems clear that [the ordinance], which provides for the posting of "No Solicitation" signs and which is not challenged in this case, coupled with the resident's unquestioned right to refuse to engage in conversation with unwelcome visitors, provides ample protection for the unwilling listener."[229] Like Justice Black in *Martin,* Justice Stevens recognized the right of individual homeowners to control the flow of information into their homes.

Therefore, in *Watchtower* the Court implicitly recognized the right for each party to control information; the canvassers need not reveal their identifying information and homeowners are able to control the flow of information into their homes. Privacy as information control was applied as the primary privacy conceptualization through which canvassers could control access to the self and homeowners could control information entering their private space.

The privacy-as-information-control conceptualization permeates Supreme Court anonymous speech cases. Individuals, whether distributing literature in public spaces or door-to-door, have a right to control the disclosure of their identities absent a compelling government interest. In each of the cases discussed above the Court recognized that

---

[228] *Watchtower*, 536 U.S. at 168-69; *id*. at 165. "Had this provision been construed to apply only to commercial activities and the solicitation of funds, arguably the ordinance would have been tailored to the Village's interest in protecting the privacy of its residents and preventing fraud. Yet, even though the Village has explained that the ordinance was adopted to serve those interests, it has never contended that it should be so narrowly interpreted."

[229] *Id.*

when individuals' identities are known, they are at a greater risk of suffering retaliatory harms. The explicit reasoning in these cases concerned the potential for these increased risk levels to chill the exercise of their First Amendment rights. Nevertheless, implicit in these decisions was the notion that individuals should determine their own level of exposure to risk, not the government. This individual determination is implemented when a privacy interest, conceptualized as information control, is exercised in order to limit access to the self or to private space.

Privacy in Anonymous Association Cases

In the anonymous speech cases examined above, the Court noted the value of anonymity in enabling free speech throughout the history of the United States and considered it an implied right protected by the First Amendment. Anonymity has also been valuable in allowing citizens to join groups that espouse unpopular ideas without fear of retaliation by the government. As Justice Arthur Goldburg once wrote, "Joining groups seems to be a passion with Americans."[230] This passion was essential to the founding of the United States. Justice Potter Stewart, in his 1963 concurrence in *Gibson v. Florida Legislative Investigation Committee*, reflected, "Like freedom of speech and a free press, the right of peaceable assembly was considered by the Framers of our Constitution to lie at the foundation of a government based upon the consent of an informed citizenry -- a government dedicated to the establishment of justice and the

[230] Gibson v. Fla. Legis. Investigation Comm., 372 U.S. 539, 564 (1963) (Douglas, J., concurring).

preservation of liberty."[231] The ability to prohibit the government from knowing one's associations has been thought to prevent a chill of the exercise of First Amendment associational rights.

There are two ways that the government can compel disclosure of one's group associations. First, the government can use laws to force groups to turn over membership lists. Rulings in these cases are a direct refutation of the privacy-as-secrecy conceptualization of privacy. In the act of joining a group, an individual entrusts his or her identity, along with other bits of personal information, to the group. As it has in the anonymous speech cases discussed above, the Court embraced the notion of limited privacy and recognized that the government can't compel individuals to disclose their membership in a group simply because a third party (the group itself) is aware of the individual's membership.[232] Second, the government can directly compel individuals to disclose their own memberships by questioning them or forcing them to testify before a public body about their involvement with a particular group.

The following analysis reveals that the Court embraced the same notions of limited privacy and privacy as a right to control information about one's self in anonymous association jurisprudence as it had in the anonymous speech cases above. The association cases provide more insight into the limits of a First Amendment right to privacy. At different points in history, certain groups like communists were considered significant internal threats to national security, and the Court considered national security

[231] Bates v. Little Rock, 361 U.S. 516, 522-23 (1960) .

[232] In the third-party doctrine, the government should be considered the second party since it is the entity attempting to access the first party's information. For instance, the government (second party) argues that it is entitled to a group member's (first party) information because the member has already shared the fact of his or her membership with the group itself (third party).

to be a sufficiently compelling state interest to justify infringement upon the individual right to control personal information.

Group Control of Member Information

The Supreme Court has protected anonymity by recognizing the right of groups to protect *parens patriae*[233] against the compelled disclosure of the identities of their members. These cases involve state and local statutes that mandated the disclosure of group membership lists, and the Court upheld the right of organizations to control access to the identities of their members. These cases differ from the pamphleteer cases in that third parties (groups) holding personal information, rather than the individual members, argued to maintain control over private information.

In *NAACP v. Alabama* , Justice John M. Harlan wrote, "This Court has recognized the vital relationship between freedom to associate and privacy in one's associations."[234] The Court reasoned, as it had in the anonymous pamphleteer cases, that individuals might be less likely to associate with others or join groups if they couldn't do so privately. The Court again embraced the notion of limited privacy as it supported an individual right to share one's personal information with one organization with the expectation that the organization would not share the information with other third parties without consent.

Two landmark anonymous association cases involved membership lists for branches of the NAACP in Alabama and Arkansas: *NAACP v. Alabama*[235] and *Bates v.*

[233] BLACK'S LAW DICTIONARY 1144 (8th ed. 2004). "The state regarded as a sovereign; the state in its capacity of provider of protection to those unable to care for themselves."

[234] 357 U.S. 449, 465 (1958).

[235] 357 U.S. 449 (1958).

Little Rock.[236] They were argued before the U.S. Supreme Court in 1958 and 1960. In *NAACP*, the Court reviewed a request by the Alabama State Attorney General's Office for "a large number of the [Alabama NAACP's] records and papers, including bank statements, leases, deeds, and records containing the names and addresses of all Alabama 'members' and 'agents' of the Association."[237] When the organization did not provide the information requested, it was found in contempt and fined. At that point the NAACP surrendered all of the requested documents except its membership lists. The organization feared that the surrendered names of individual members might somehow be leaked to private citizens who might decide to harm NAACP members.

In 1958 the Civil Rights Movement was underway and building momentum, which increased racial tensions in the South.[238] Justice John M. Harlan wrote for the Court that his decision to overturn the contempt charge was based primarily on the NAACP's demonstration that disclosing the names of members in Alabama would place those individuals at risk.[239] Justice Harlan recognized that members who were identified

---

[236] 361 U.S. 516 (1960).

[237] *NAACP*, 357 U.S. at 453. The request was part of a discovery process stemming from a case involving the NAACP's appeal of an injunction that had been filed to stop the organization from conducting business for alleged noncompliance with an Alabama statute that required businesses and organizations from outside the state to qualify by "filing its corporate charter with the Secretary of State and designating a place of business and an agent to receive service of process;" *see* ALA. CODE, 1940, Tit. 10, §§ 192-198. The NAACP alleged that it was not subject to the qualification statute because it was a nonprofit organization, and it moved to quash the enjoinder that the State Attorney General had obtained for the organization's failure to comply.

[238] For a complete timeline of the Civil Rights Movement (1954-2005) visit: http://www.infoplease.com/spot/civilrightstimeline1.html.

[239] *NAACP*, 357 U.S. at 462 63. Justice Harlan wrote: "Under these circumstances, we think it apparent that compelled disclosure of petitioner's Alabama membership is likely to affect adversely the ability of petitioner and its members to pursue their collective effort to foster beliefs which they admittedly have the right to advocate, in that it may induce members to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure."

might be exposed to "economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility."[240] His concern was not that the State of Alabama would directly retaliate against those advocating for racial equality. Instead, he feared that once released, the membership list might be leaked to private citizens. He wrote, "The crucial factor is the interplay of governmental and private action, for it is only after the initial exertion of state power represented by the production order that private action takes hold."[241]

Justice Harlan cited language from the 1950 case *American Communications Association v. Douds*,[242] which asserted that a statute need not directly threaten members of a group to be constitutionally infirm. In *Douds*, the Court wrote: "[T]he fact that no direct restraint or punishment is imposed upon speech or assembly does not determine the free speech question. Under some circumstances, indirect 'discouragements' undoubtedly have the same coercive effect upon the exercise of First Amendment rights as imprisonment, fines, injunctions or taxes."[243] Similarly, Justice Harlan considered the threat of retaliatory harms against exposed Alabama NAACP members an "indirect discouragement" of free association. [244]

---

[240] *Id.* at 462.

[241] *Id.* at 463. Today the situation is reversed. The government can access information collected in the private sector and potentially "harm" citizens as a result of misidentifying them as terror suspects in data mining programs.

[242] Am. Commc'n Ass'n v. Douds, 339 U.S. 382 (1950).

[243] *Id.* at 403. This was a labor case in which officers of a Labor Union were required to submit affidavits attesting to the fact that they were not members of the Communist Party.

[244] *NAACP*, 357 U.S. at 460. "Petitioner argues that in view of the facts and circumstances shown in the record, the effect of compelled disclosure of the membership lists will be to abridge the rights of its rank-and-file members to engage in lawful association in support of their common beliefs. It contends that governmental action which, although not directly suppressing association nevertheless carries this consequence, can be justified only upon some overriding valid interest of the State."

As established in the preceding analysis of anonymous speech cases, as the level of risk to those exercising their First Amendment rights increases, so too does their privacy interest in controlling personal information. In 1958 the level of risk to individuals advocating racial equality in the South was deemed significant. Only a compelling government interest in disclosure could justify infringement upon the right of the NAACP to control identifying information on behalf of its members. The State of Alabama's desire to include a membership list in an organization's charter did not represent such a compelling state interest.

The right of the NAACP to control the personal information of its members was again supported in *Bates v. Little* Rock.[245] In 1960 the Court reviewed two Arkansas city ordinances under which local governments sought to compel the NAACP to surrender membership lists. Two municipalities, Little Rock and North Little Rock, had identical ordinances[246] that allowed them to levy taxes on any person, firm, individual, or corporation engaging in trade, business, profession, vocation or calling within their corporate limits. Charitable organizations like the NAACP were exempted from the ordinances until 1957, when amendments to the ordinances required such organizations operating within city limits to provide, among other information, "a statement as to dues, assessments, and contributions paid … [and] by whom."[247] Furthermore, the ordinances

---

[245] 361 U.S. 516 (1960).

[246] LITTLE ROCK ORD. NO. 7444; NORTH LITTLE ROCK ORD. No. 1786.

[247] *Bates*, 361 U.S. at 518. Altogether, the ordinances required six types of information: "(1) the official name of the organization; (2) its headquarters or regular meeting place; (3) the names of the officers, agents, servants, employees, or representatives, and their salaries; (4) the purpose of the organization; (5) a statement as to dues, assessments, and contributions paid, by whom and when paid, together with a statement reflecting the disposition of the funds and the total net income; (6) an affidavit stating whether the organization is subordinate to a parent organization, and if so, the latter's name."

explicitly stated that all the information collected would be public and made available to "any interested party at all reasonable business hours."[248] Justice Potter Stewart seems to have considered this latter provision to be the same type of "indirect discouragement" discussed in *Douds* and considered by Justice Harlan in *NAACP*.[249]

Daisy Bates was the custodian of records in the Little Rock branch of the NAACP, and Birdie Williams held the same position for the North Little Rock branch. Both refused to disclose their membership lists. In the Bates trial, evidence was introduced by the NAACP "to show that many former members of the local organization had declined to renew their membership because of the existence of the ordinance in question."[250] Atthe Williams trial , evidence was entered thatdemonstrated that "those who had been publicly identified in the community as members of the National Association for the Advancement of Colored People had been subjected to harassment and threats of bodily harm."[251] Bates and Williams were both convicted at trial and their cases were combined on appeal.

Justice Potter Stewart wrote for the majority in *Bates*, and both convictions were overturned.[252] In language similar to the "indirect discouragements" discussed in *Douds*, Justice Stewart noted, "Freedoms such as [anonymous assembly] are protected not only

---

[248] *Id.*

[249] *Id.* at 523-24.

[250] *Id.* at 521.

[251] *Id.* at 521-22.

[252] *Id*. at 527. "We conclude that the municipalities have failed to demonstrate a controlling justification for the deterrence of free association which compulsory disclosure of the membership lists would cause. The petitioners cannot be punished for refusing to produce information which the municipalities could not constitutionally require. The judgments cannot stand."

against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference."[253] The municipalities argued that they had a right to tax, but the Court, having established that the ordinances were a significant infringement on associational rights, ruled that the right to tax is not a sufficiently compelling state interest to justify the infringement.

In both *NAACP* and *Bates*, the Court granted the control of personal information to groups in situations where there was a serious threat of harm to individual members if their identities were disclosed. Conversely, the Court has ruled that the government can compel the surrender of lists of campaign donors absent such potential harms if the government can demonstrate a compelling interest and the disclosure is narrowly tailored. In one such case, *Buckley v. Valeo*,[254] the Court reviewed challenges made by several plaintiffs regarding the constitutionality of the Federal Election Campaign Act of 1971 as amended in 1974.[255] The reporting and disclosure requirements of the Act were challenged in particular as an abridgement of the First Amendment right of anonymous association.

When considered from a privacy perspective, the question becomes a matter of information control. Many individuals join others of like mind in financially supporting particular candidates, parties, or issues. This is association, and individuals may have a privacy interest in not disclosing the amount of their contributions and the groups they

[253] *Id.* at 523.

[254] 424 U.S. 1 (1976).

[255] 2 U.S.C. § 431 et seq. (1970 ed., Supp. IV).

support. In *Buckley* the Court had to decide whether individuals had the right to control information regarding their donations to political campaigns.

The Court ruled that disclosure of contributions would likely not result in the type of harms the Court sought to avoid in *NAACP*, but it did recognize the potential chill on First Amendment political association. It held: "It is undoubtedly true that public disclosure of contributions to candidates and political parties will deter some individuals who otherwise might contribute. In some instances, disclosure may even expose contributors to harassment or retaliation."[256] Such a chill would likely harm smaller political parties in particular. The Court noted: "These movements are less likely to have a sound financial base and thus are more vulnerable to falloffs in contributions. In some instances fears of reprisal may deter contributions to the point where the movement cannot survive."[257] Nevertheless, the Court ultimately held that the disclosure requirements were constitutional because the appellants could only "offer the testimony of several minor-party officials that one or two persons refused to make contributions because of the possibility of disclosure."[258]

In *Buckley*, the Court recognized that the government had a substantial interest in disclosure thatwas evident in the legislative history of the Act. The government reasoned that disclosure of campaign contributions informs the electorate as to the source and allocation of a candidate's money, may deter actual corruption and avoid the appearance of corruption, and provides a means of gathering the data necessary to detect violations of

[256] *Buckley*, 424 U.S. at 68.

[257] *Id*. at 71.

[258] *Id*. at 71 72.

contribution limitations.[259] These interests, absent the type of potential harm recognized in *NAACP* and *Bates,* were found to justify infringements upon the right to anonymous association.

Compelled Testimony about Group Membership

Another way for the government to discover whether someone is a member of a group is through direct interrogation of suspected members. Whereas the Court supported the right of canvassers and pamphleteers to control the disclosure of their identities in the face of legislative interests such as the prevention of littering, fraud prevention, and homeowner privacy, it held that the government could compel the disclosure of personal information when facing a perceived national security threat such as Communism.

In 1959 the Supreme Court limited the right of anonymous association in *Barenblatt v. United States.*[260] This case dealt with compelled testimony from a witness before the House Committee on Un-American Activities (HUAC).[261] Lloyd Barenblatt was a college professor suspected of having associated with a Communist-front organization while a graduate student at the University of Michigan. Barenblatt was summoned before HUAC and asked to reveal whether he was or ever had been a member of the Communist Party. He was also asked to reveal the identities of anyone else he

[259] *Id*. at 66 68.

[260] 360 U.S. 109 (1959).

[261] *See generally* VICTOR S. NAVASKY, NAMING NAMES (3d ed. 2003) (providing a general description of the committee and an overview of its history).

knew who was or had been a member of the Communist Party. Barenblatt refused and was held in contempt of Congress.

Justice Harlan wrote the opinion in *Barenblatt*, an opinion thatneeds to be evaluated within its historical context. A number of events in the 1950s -- the Korean War, the McCarthy hearings, and the acquisition of the hydrogen bomb by the U.S.S.R. -- had elevated the threat of Communism in the public consciousness. By 1959, the internal and external threats posed by Communism were considered national security priorities, and thus preventing Communist infiltration of organizations and industries inside the United States was considered a compelling state interest.

Justice Harlan, referring to his earlier opinion in *NAACP*, wrote: "Undeniably, the First Amendment in some circumstances protects an individual from being compelled to disclose his associational relationships. However, the protections of the First Amendment . . . do not afford a witness the right to resist inquiry in all circumstances."[262] Thus, along with protecting the integrity of the election process as established in *Buckley*, domestic intelligence gathering about specific groups thought to pose an internal security threat to the United States justifies a suspension of the individual privacy right to control personal information.

Justice Harlan acknowledged "the interest of the people as a whole in being able to join organizations, advocate causes and make political 'mistakes' without later being subjected to governmental penalties for having dared to think for themselves."[263] Individuals publicly identified as Communists by HUAC in the late 1950s were barred

[262] *Barenblatt*, 360 U.S. at 126.

[263] *Id.* at 144 (Black, J., dissenting).

from government employment, may have had difficulty securing employment in the private sector, and might have been shunned socially. Nevertheless, the potential harms resulting from disclosure did not rise to level of those he had considered in *NAACP*. Justice Harlan ruled that Baranblatt's contempt conviction was constitutional as Congress was within its historical and legislative authority to investigate how far into the United States university system Communists had infiltrated. The Court ruled that the threat of Communists taking down the U.S. Government was sufficiently compelling to survive scrutiny.

In 1963, a Florida state legislative committee empowered to investigate subversive and Communist activities tried to compel the Miami branch of the NAACP to disclose its membership lists so that the committee could determine whether known Communists were members of the organization.[264] Justice Arthur Goldburg wrote the majority opinion in *Gibson v. Florida Legislative Investigation Committee*, [265]and the Court ruled that the NAACP need not disclose its membership lists.

Using language similar to that in *NAACP* and *Bates*, Justice Goldburg wrote that anonymous association rights are "all the more essential here, where the challenged privacy is that of persons espousing beliefs already unpopular with their neighbors and the deterrent and 'chilling' effect on the free exercise of constitutionally enshrined rights

[264] Gibson v. Fla. Legis. Investigation Comm., 372 U.S. 539, 548 (1963). "[The] record indicates that the association was and is against communism and has voluntarily taken steps to keep Communists from being members. Each year since 1950, the N.A.A.C.P. has adopted resolutions barring Communists from membership in the organization. Moreover, the petitioner testified that all prospective officers of the local organization are thoroughly investigated for Communist or subversive connections and, though subversive activities constitute grounds for termination of association membership, no such expulsions from the branch occurred during the five years preceding the investigation."

[265] 372 U.S. 539 (1963). In 1957 the State sought to compel the disclosure of the Miami branch membership lists. When the NAACP refused, Florida sought a court order, which was fought by the NAACP. This action started the judicial procedure that was under review in *Gibson*.

of free speech, expression, and association is consequently the more immediate and substantial."[266] Despite the national security threat posed by Communism in the early 1960s, in *Gibson* the Court ruled that Florida's desire to link Communists to legitimate, if regionally unpopular, groups did not justify government intrusion upon individual associational rights. In his concurrence in *Gibson,* Justice Douglas referred to Justice Harlan's decision in *NAACP*. He wrote:

> The right of association has become a part of the bundle of rights protected by the First Amendment, and the need for a pervasive right of privacy against government intrusion has been recognized, though not always given the recognition it deserves. Unpopular groups like popular ones are protected. Unpopular groups if forced to disclose their membership lists may suffer reprisals or other forms of public hostility. But whether a group is popular or unpopular, the right of privacy implicit in the First Amendment creates an area into which the Government may not enter.[267]

What distinguishes *Gibson* from *Barenblatt* is that in *Barenblatt* the individual being interrogated was suspected of participating in subversive activities. In *Gibson,* the privacy and associational rights of individuals not suspected of any wrongdoing were being infringed by a government body investigating individuals already identified as subversives. Justice Douglas asserted: "One man's privacy may not be invaded because of another's perversity. If the files of the NAACP can be ransacked because some Communists may have joined it, then all walls of privacy are broken down."[268] Justice

---

[266] *Id.* at 556-57.

[267] *Id.* at 569-70 (Douglas, J., concurring).

[268] *Id.* at 572 (Douglas, J., concurring).

Douglas indicated that associational privacy can be constitutionally invaded when a particular individual is suspected of a crime. He wrote:

> Whether the problem involves the right of an individual to be let alone in the sanctuary of his home or his right to associate with others for the attainment of lawful purposes, the individual's interest in being free from governmental interference is the same, and, except for the limited situation where there is "probable cause" for believing that he is involved in a crime, the government's disability is equally complete.[269]

The Court's primary conceptualization of privacy in anonymous association cases has been the same as in anonymous speech cases: privacy as information control. In both types of cases the Court recognized that in order to protect anonymity under the First Amendment, it must accept the idea that individuals, or groups acting on behalf of their individual members, have a right to control the disclosure of identity. *Barenblatt* established that this right is limited and if the government is able to demonstrate a compelling state interest, such as a national security threat, then it is constitutional for the government to compel disclosure.

As it had in the anonymous speech cases, the Court recognized that when individuals' identities are known, they may perceive themselves to be at risk of suffering retaliatory harms. This perception might make individuals less likely to join groups or associate with those who hold beliefs similar to their own. This would be a chill on the exercise of their First Amendment rights. Explicit and implicit in these anonymous association decisions was the notion that individuals, or groups on their behalf, should have the right to determine their own level of exposure to risk, not the government.

[269] *Id.* at 570, n7 (Douglas, J., concurring).

First Amendment Privacy and Surveillance

The Court has ruled that, absent a compelling state interest, when legislative bodies attempt to compel the disclosure of either membership lists or individual testimony as to group membership, individuals and groups have an implied First Amendment right to anonymity. This right was conceptualized as a right for individuals, or groups on behalf of individuals, to control access to identifying information by the government. Nevertheless, there is another method that has been utilized by the government to identify members of groups espousing unpopular or dissident beliefs. The government can simply observe or infiltrate groups and then record the names of group members and track group activities.

The Court had an opportunity in 1972 to apply the privacy conceptualization it had used in cases like *Tally*, *McEntyre*, *NAACP*, and *Gibson* to the U.S. Army domestic surveillance program, which had been in operation since 1967. Even though *Laird v. Tatum*[270] was decided on a procedural issue, plaintiffs' lack of standing, the Court discussed at length whether domestic surveillance might cause a chill on First Amendment rights to assemble anonymously.

What distinguished *Laird* from the anonymous speech and association cases previously discussed is that the Court did not recognize an alleged chilling effect on a group's association rights to be sufficient grounds upon which to mount a constitutional challenge. In anonymous speech cases, the Court reasoned that individuals might be less likely to participate in the marketplace of ideas if they had to disclose their identities to others and thereby place themselves at risk. In anonymous association cases, the Court

[270] 408 U.S. 1 (1972).

recognized that members of groups that espoused unpopular beliefs might be at risk of retaliatory actions by others if their identities were known. Fear of such retaliations might chill the desire of individuals to associate with such groups. The question of privacy in one's associations was never reached by the Court in the landmark surveillance case decided in 1972.

Writing for the Court in *Laird,* Chief Justice Warren E. Burger ruled that the "subjective chill" that resulted from fear that information collected by the government might someday be used to harm those about whom the information had been collected was not a sufficient justification to issue an injunction against domestic intelligence operations conducted by the U.S. Army.[271] In 1967 the U.S. Army was deployed to Detroit to assist state and local law enforcement in handling a series of race riots. Afterward, the Army developed a plan to collect information on those individuals and groups most likely to be involved in future demonstrations.[272] It was thought that this would help the Army identify situations most likely to turn violent.[273]

Thus, in 1968 and 1969 the Department of the Army was engaged in "surveillance of lawful and peaceful civilian activity" in an effort to attain "information relating to potential or actual civil disturbances (or) street demonstrations."[274] The information was

---

[271] *Id.* at 13-14. "Allegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm."

[272] *Id.* at 24-25 (Douglas, J., dissenting). Groups under surveillance when this case was filed included: the Southern Christian Leadership Conference, Clergy and Laymen United against the War in Vietnam, the American Civil Liberties Union, Women's Strike for Peace, and the NAACP.

[273] *Id.* at 2 (holding that "Since the Army is sent into territory almost invariably unfamiliar to most soldiers and their commanders, their need for information is likely to be greater than that of the hometown policeman"); *id.* at 5-6 (reasoning that "When force is employed it should be intelligently directed, and this depends upon having reliable information--in time").

[274] *Id*. at 2.

collected from the news media and other publications and from Army agents who attended public meetings. Field reports were submitted by the agents "describing the meetings, giving such data as the name of the sponsoring organization, the identities of speakers, the approximate number of persons in attendance, and an indication of whether any disorder occurred."[275]

The intelligence information was then sent to Fort Holabird, Maryland, where it was stored on computer tape and then disseminated to bases around the country.[276] Members of the Central Committee of Conscientious Objectors filed suit to challenge the constitutionality of this Army surveillance system. The plaintiffs did not show any evidence of having suffered direct harms or monetary damages but instead insisted that a "deprivation of fundamental constitutional rights of intangible value [was] involved."[277] Unlike the decisions in *NAACP* and *Bates*, the Court had no evidence that innocent individuals had been harmed because the Army was aware of their membership in certain groups or of their participation in demonstrations.[278] The Army did modify its intelligence program as a result of the case, but the Court never concluded whether the program constituted a direct infringement on First Amendment rights.

---

[275] *Id.* at 6; *See also id.* at 24-25 (Douglas, J., dissenting) (noting that "The Army uses undercover agents to infiltrate these civilian groups and to reach into confidential files of students and other groups. The Army moves as a secret group among civilian audiences, using cameras and electronic ears for surveillance"): *id.* at 26-27 (Douglas, J., dissenting) (noting also that "[T]he Army's surveillance was not collecting material in public records but staking out teams of agents, infiltrating undercover agents, creating command posts inside meetings, posing as press photographers and newsmen, posing as TV newsmen, posing as students, and shadowing public figures").

[276] *Id.* at 6.

[277] Tatum v. Laird, 444 F.2d 947, 950 (C.A.D.C. Apr. 27, 1971).

[278] *Laird*, 408 U.S. at 8. "It was the view of the district court that respondents failed to allege any action on the part of the Army that was unlawful in itself and further failed to allege any injury or any realistic threats to their rights growing out of the Army's actions."

Justice William O. Douglas wrote a dissent in *Laird* in which he argued that the need to show harm should not have been central to the Court's review of an Army domestic intelligence program. He wrote: "One need not wait to sue until he loses his job or until his reputation is defamed. To withhold standing to sue until that time arrives would in practical effect immunize from judicial scrutiny all surveillance activities, regardless of their misuse and their deterrent effect."[279] Justice Douglas argued that Army surveillance is counter to the very principles of the Constitution. He asserted:

> The Bill of Rights was designed to keep agents of government and official eavesdroppers away from assemblies of people. The aim was to allow men to be free and independent and to assert their rights against government. There can be no influence more paralyzing of that objective than Army surveillance. When an intelligence officer looks over every noncomformist's shoulder in the library, or walks invisibly by his side in a picket line, or infiltrates his club, the America once extolled as the voice of liberty heard around the world no longer is cast in the image which Jefferson and Madison designed, but more in the Russian image.[280]

Justice Douglas would have preferred the Court move beyond the issue of standing and apply a substantive review of domestic surveillance. It remains to be seen if the Court will adopt the same conceptualizations of privacy in surveillance cases as it has in anonymous speech and assembly cases.

Privacy under the First Amendment

The primary privacy conceptualization embraced by the Court in First Amendment jurisprudence is privacy as information control. Using historical examples,

---

[279] *Id.* at 26 (Douglas, J., dissenting).

[280] *Id.* at 28-29 (Douglas, J., dissenting).

the Court has established the substantive value of anonymity to free speech and association especially in regard to individuals and groups espousing unpopular or dissident ideas. Anonymity is the ability to keep one's identity private even if other aspects of one's personality, such as political or religious affiliation, have already been disclosed. This notion of sharing only some aspects of one's identity is referred to as limited privacy and the Court has supported this idea as central to the right to speak or associate anonymously.

Other conceptualizations of privacy discussed in Chapter One, namely privacy-as-access-to-self and privacy-as-space, emerge in First Amendment privacy jurisprudence as privacy interests that have been subsumed under the broader umbrella of the privacy-as-information-control conceptualization. For example, in *Watchtower* the Court recognized the right of homeowners to protect their home as private space, yet the concept of spatial privacy was discussed in terms of the homeowners' ability to control the flow of information into their homes. *McEntyre* provided a similar example. The Court reasoned that persuasive, political pamphlets would likely contain information that might provide insight into a pamphleteer's deeply held faiths or beliefs. This information, when combined with the compelled disclosure of identity, could provide an unwarranted glimpse of an individual's inviolate personality, his or her self. Nevertheless, the Court reasoned that this privacy interest could be protected by recognizing that individuals have the right to control access to their identifying information.

CHAPTER III

PRIVACY AND THE FOURTH AMENDMENT

Since, dataveillance is about government access to information that citizens have shared with others in order to participate in daily life, the Court's conceptualizations of privacy in First Amendment privacy jurisprudence will be helpful when evaluating KDD dataveillance from an access perspective. However, the purpose for accessing such information in the case of KDD dataveillance is for the government to identify potential criminal suspects. Therefore, understanding how the Supreme Court has conceptualized privacy in Fourth Amendment privacy jurisprudence is also necessary when determining if the Court's current privacy conceptualizations will protect privacy rights against infringement by federal KDD dataveillance programs.

The U.S. Supreme Court has held that the "well-known historical purpose of the Fourth Amendment, directed against general warrants and writs of assistance, was to prevent the use of governmental force to search a man's house, his person, his papers, and his effects, and to prevent their seizure against his will."[281] It was a common practice

---

[281] Olmstead v. United States, 277 U.S. 438, 463 (1928). *See also* Boyd v. United States, 116 U.S. 616, 624-26 (1886) (explaining how the British used writs of assistance to search private property for stolen goods and defining "the practice of issuing general warrants by the secretary of state, for searching private houses for the discovery and seizure of books and papers that might be used to convict their owner of the charge of libel" as a "grievous abuse"); Weeks v. United States, 232 U.S. 383, 390 (1914) (asserting that resistance to general warrants and writs or assistance "had established the principle which was enacted into the fundamental law in the 4th Amendment, that a man's house was his castle, and not to be invaded by any general authority to search and seize his goods and papers").

during the colonial period for royal governors, when seeking evidence of a crime, to send members of the militia to forcibly invade a person's home and seize material that might be used against thatperson at trial. The Fourth Amendment, when ratified in 1791, limited government's power to invade privately held property by requiring due process.[282] The actual language of the Amendment explicitly limited government access to material items and property but did not mention the more substantive notion of "privacy" or the right of citizens to be left alone.[283]

This chapter's examination of the Supreme Court's language in Fourth Amendment privacy jurisprudence reveals an evolutionary process through which the Court gradually moved beyond the colonial, property-based conceptualization of Fourth Amendment privacy and ultimately developed a broader doctrine. This evolution involved four stages of privacy conceptualizations: privacy as Fourth and Fifth Amendment procedural due process, privacy as space, privacy as secrecy, and the current stage in which the Court recognizes privacy as information control. The privacy doctrine was somewhat technologically determined. The continuing development and application of new surveillance technologies propelled the Court's understanding of Fourth Amendment privacy through each of these stages.

The Founders were initially concerned about the government's ability to enter upon private property for the purpose of collecting evidence that could be used against the property owner in a criminal trial. This use of the contents of citizens' own homes,

[282] BLACK'S LAW DICTIONARY 539 (8th ed. 2004). Due process is defined as: "The minimal requirements of notice and a hearing guaranteed by the Due Process Clauses of the Fifth and Fourteenth Amendments, esp. if the deprivation of a significant life, liberty, or property interest may occur."

[283] U.S. CONST. amend. IV. "The Right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

papers, and effects amounted to a form of self-incrimination. Thus, in the late eighteenth and throughout the nineteenth century, the Court's concept of Fourth Amendment protection was about the admissibility of evidence and was often closely connected to Fifth Amendment due process protection.

Proper procedure under the Fourth Amendment required that the government show probable cause and secure a warrant. When it was determined that evidence had been secured in violation of the Fourth Amendment, that evidence was not admissible in court as this would be considered a violation of one's Fifth Amendment right against self-incrimination. At this stage Fourth Amendment privacy protections were about procedure.

The twentieth century brought new surveillance technologies such as wire taps, bugging devices, aircraft, and thermal imagers. These technologies enabledaw enforcement officers to gather incriminating evidence from personal spaces without physical trespass. This forced the Court to move beyond procedure and grapple with the nature of privacy as protected by the Fourth Amendment.

Thus, in the second stage, the Court embraced the privacy-as-space conceptualization and required due process in the form of a search warrant whenever law enforcement personnel trespassed upon private property. Evidence collected through the use of technology that did not require physical trespass, like wire tapping, was admissible. As such technology became more common and more powerful, it became harder to anchor individual privacy interests in physical space.

During the third stage, the Court reduced its emphasis on physical trespass and focused instead upon whether an individual had created a reasonable expectation of

privacy in the material or information seized. In doing so, the Court recognized the privacy-as-secrecy conceptualization in the Fourth Amendment privacy doctrine. Individuals were expected to have taken some measures (personal agency) intended to conceal information from others. Information that was willingly shared with third parties was no longer considered private (third-party doctrine).

Ultimately, new surveillance technologies prevented individuals from taking steps toward creating an expectation of privacy in spaces, activities, or information, and the role of personal agency was negated. As individuals were no longer capable of defending their own privacy interests, the Court implicitly recognized that constitutional protections needed to fill the gap. This is when the Court adopted the privacy-as-information-control conceptualization. The following case analysis details the evolution of the Court's conceptualization of privacy under the Fourth Amendment.

Due Process and the Fourth and Fifth Amendments

Fourth Amendment protections were initially considered in combination with the due process requirements of the Fifth Amendment.[284] In *Boyd v. United States*[285] the

[284] U.S. CONST. amend. V. The Fifth Amendment reads in part: "No person . . . shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

[285] 116 U.S. 616 (1886). In this case the defendant was accused of using illegal means to avoid paying customs duties on imported plate glass. The prosecution relied on statutory authority to compel the defendant to produce invoices and other papers that would establish the value of 29 sheets of plate glass. This information would be used to build the case against the defendant. The defendant in the case appealed on the grounds that the statute, enacted during the Civil War, was an infringement of his Fourth and Fifth Amendment rights.

Court explained how the Fourth and Fifth Amendments run "almost into each other."[286] Justice Joseph P. Bradley wrote:

> They throw great light on each other. For the "unreasonable searches and seizures" condemned in the fourth amendment are almost always made for the purpose of compelling a man to give evidence against himself, which in criminal cases is condemned in the fifth amendment; and compelling a man "in a criminal case to be a witness against himself," which is condemned in the fifth amendment, throws light on the question as to what is an "unreasonable search and seizure" within the meaning of the fourth amendment.[287]

In *Boyd*, the Court struck down a federal statute that had been enacted and amended between 1863 and 1874 and enabled state attorneys general to compel suspects to produce documents, such as shipping invoices or receipts, which could be used as evidence against them in trial. If the defendants refused, this failure to produce the records was considered an admission of guilt.[288]

Justice Bradley held in *Boyd* that the statute was repugnant to both the Fourth and Fifth Amendments.[289] *Boyd* established that "constitutional liberty and security" protected by these amendments "apply to all invasions on the part of the government and

---

[286] *Id.* at 630.

[287] *Id.* at 633.

[288] *Id.* at 621. Justice Bradley noted: "It was the first legislation of the kind that ever appeared on the statute book of the United States, and, as seen from its date, was adopted at a period of great national excitement, when the powers of the government were subjected to a severe strain to protect the national existence."

[289] *Id.* at 621-22. Justice Bradley wrote that such a statute had the same effect as would the use of government agents to physically break into a suspect's home and search and seize incriminating evidence. Bradley wrote: "[The statute] declares that if he does not produce them, the allegations which it is affirmed they will prove shall be taken as confessed . . . . It is true that certain aggravating incidents of actual search and seizure, such as forcible entry into a man's house and searching among his papers, are wanting . . . but it accomplishes the substantial object of those acts in forcing from a party evidence against himself. It is our opinion, therefore, that a compulsory production of a man's private papers to establish a criminal charge against him, or to forfeit his property, is within the scope of the fourth amendment to the constitution, in all cases in which a search and seizure would be, because it is a material ingredient, and effects the sole object and purpose of search and seizure."

its employees of the sanctity of a man's home and the privacies of life."[290] Justice Bradley used broad language to define the liberty interests these amendments protected: "It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property.[291]

Between *Boyd* and the next landmark Fourth Amendment decision in 1928, *Olmstead v. United States,*[292] Fourth Amendment cases primarily dealt with the question of whether due process, in the form of a warrant,[293] was necessary in a particular circumstance and whether it had been provided. In the 1914 case of *Weeks v. United States*,[294] the Court explicitly defined the effect of the Fourth Amendment as

> to put the courts of the United States and Federal officials, in the exercise of their power and authority, under limitations and restraints as to the exercise of such power and authority, and to forever secure the people, their persons, houses, papers, and effects, against all unreasonable searches and seizures under the guise of law.[295]

Thus, according to *Weeks*, an unreasonable (unconstitutional) search or seizure was one conducted without due process. The limitation or restraint upon government power was understood to be the warrant requirement, which would provide judicial oversight of any

---

[290] *Id*. at 630.

[291] *Id.*

[292] 277 U.S. 438 (1928).

[293] BLACK'S LAW DICTIONARY 1616 (8th ed. 2004) (defining a warrant as "a writ directing or authorizing someone to do an act, esp. one directing a law enforcer to make an arrest, a search, or a seizure"); *id.* at 1379 (defining a search warrant as "a judge's written order authorizing a law enforcement officer to conduct a search of a specified place and to seize evidence").

[294] 232 U.S. 383 (1914).

[295] *Id.* at 391-92.

government intrusion upon private space and of government seizures of private papers or effects.

In 1920, the Court ruled that papers that had been seized without a warrant from a defendant's office while he was being detained by law enforcement officials had been seized without "a shadow of authority."[296] The papers were returned to the defendant and could not be used as evidence at trial.[297] In 1921, the Court ruled that a suspect's Fourth Amendment rights were violated when revenue officers "coerced" his wife into allowing them to enter and search her home without a warrant.[298] That same year, the Court ruled that a U.S. Army private violated a defendant's Fourth Amendment rights when he pretended "to make a friendly call on …[the defendant], gained admission to his office, and in his absence, without warrant of any character, seized and carried away several documents."[299]

In each of these instances materials were gathered without a warrant or subpoena, and since the suspect of the investigation was denied due process, the evidence gathered unconstitutionally was considered inadmissible in court. Combining Fourth and Fifth Amendment review was understandable since the Court never had to deal with a method of searching or seizing that didn't involve physical trespass; admissibility hinged upon

---

[296] Silverthorne Lumber Co. v. United States, 251 U. S. 385, 390 (1920). The district attorney provided subpoenas for certain materials thought to be central to the prosecution's cases, but not until after the defendant filed to have the materials returned. The Court ruled that the materials needed to be returned and could not be used at trial

[297] Again, Fifth Amendment protections were applied directly as a result of a Fourth Amendment violation as was established in *Boyd*. This tendency to hold inadmissable any evidence gained through a violation of the Fourth Amendment was termed the "exclusionary rule." *See* BLACK'S LAW DICTIONARY 606, NO. 2 (8th ed. 2004) (defining the exclusionary rule as "A rule that excludes or suppresses evidence obtained in violation of an accused person's constitutional rights").

[298] Amos v. United States, 255 U.S. 313, 317 (1921).

[299] Gouled v. United States, 255 U.S. 298, 304 (1921).

the presence of procedural due process. Eventually, technology allowed the government to gather evidence from within private spaces without physical trespass, and at that point the Court was forced to conduct a more substantive Fourth Amendment analysis regarding what constituted constitutionally protected space.

Privacy as Space

In the 1928 landmark case *Olmstead v. Unites States*,[300] Chief Justice Howard Taft explicitly separated Fifth and Fourth Amendment analyses when he wrote, "There is no room in the present case for applying the Fifth Amendment, unless the Fourth Amendment was first violated."[301] This language began a new Fourth Amendment doctrine, which was limited to the question of whether a particular search or seizure was constitutional. Chief Justice Taft's analysis was influenced by the previously mentioned *Weeks v. United States*,[302] in which the Court ended what Taft referred to as a "phase" during which the government misused its power of compulsion and the trial courts failed to question the method used by the government to obtain evidence whenever the evidence was considered relevant to a criminal trial.[303] He wrote:

---

[300] 277 U.S. 438, 462 (1928).

[301] *Id.* at 462. He also noted, "There was no evidence of compulsion to induce the defendants to talk over their many telephones." Thus, for Chief Justice Taft, the Fourth Amendment protections were limited to due process in cases wherein the government had to conduct a physical trespass while collecting evidence, and Fifth Amendment analysis was limited to whether defendants were compelled to provide evidence against themselves. After *Olmstead*, the Court no longer enmeshed Fourth and Fifth Amendment analysis together.

[302] 232 U.S. 383 (1914). This case involved an individual accused of conducting illegal gambling (lottery and betting) operations. The defendant was arrested without a warrant, and, while he was in custody, the police searched his residence twice without a warrant. Both times the police confiscated papers and materials as evidence.

[303] *Olmstead*, 277 U.S. at 463-64. *See also Weeks*, 232 U.S. at 388 (explaining that upon consideration of the petition filed for a return of the property so seized, the court ordered the return of the material that was

> The striking outcome of the *Weeks* case and those which followed it was the sweeping declaration that the Fourth Amendment, although not referring to or limiting the use of evidence in court, really forbade its introduction, if obtained by government officers through a violation of the amendment. Theretofore many had supposed that under the ordinary common-law rules, if the tendered evidence was pertinent, the method of obtaining it was unimportant.[304]

Weeks prioritized Fourth Amendment analysis because after this landmark decision, the ultimate success of a criminal prosecution depended upon the procedure used by law enforcement in procuring evidence. The process could no longer be ignored in court. As held by Justice William R. Day in *Weeks*:

> If letters and private documents can thus be seized and held and used in evidence against a citizen accused of an offense, the protection of the 4th Amendment, declaring his right to be secure against such searches and seizures, is of no value, and, so far as those thus placed are concerned, might as well be stricken from the Constitution.[305]

Weeks established the importance of Fourth Amendment protections, but it was the *Olmstead* decision that anchored Fourth Amendment due process to the notion of private space. Central to Chief Justice Taft's Fourth Amendment analysis was a determination of whether government agents had committed trespass by entering a private space without a warrant in the process of collecting evidence.

---

not pertinent to the charge against the defendant, but denied the petition "as to pertinent matter, reserving the right to pass upon the pertinency at a later time" and that the district attorney "returned part of the property taken, and retained the remainder, concluding a list of the latter with the statement that, 'all of which last above described property is to be used in evidence in the trial of the above-entitled cause, and pertains to the alleged sale of lottery tickets of the company above named'").

[304] *Olmstead*, 277 U.S. at 462-63.

[305] 232 U.S. at 388. "The efforts of the courts and their officials to bring the guilty to punishment, praiseworthy as they are, are not to be aided by the sacrifice of those great principles established by years of endeavor and suffering which have resulted in their embodiment in the fundamental law of the land."

In *Olmstead*, law enforcement agents tapped the phone lines leading from the private homes and offices of a number of suspects accused of running a sizable import business in violation of the National Prohibition Act.[306] No law enforcement officers actually entered upon private property while setting up the taps. The office lines were tapped in the basement of the large building in which the offices were located, and the home lines were tapped from utility poles located in the public streets near each residence.

The Court reviewed the procedure followed by law enforcement in accessing the targeted conversations, and the review necessarily included a consideration of the nature of the evidence in question. Chief Justice Taft reasoned that intercepting electronic information outside of a private space is something different than physically entering a property for the purpose of listening to a conversation or of confiscating material objects. Chief Justice Taft asserted:

> The [Fourth] amendment itself shows that the search is to be of material things -- the person, the house, his papers, or his effects. The description of the warrant necessary to make the proceeding lawful is that it must specify the place to be searched and the person or things to be seized.[307]

It cannot be said that the information exchanged in a telephone call is material or that a stream of electronic pulses is a place. In essence, a phone call is personal information that is being delivered via a third party, much like a piece of mail.

---

[306] *Olmstead*, 277 U.S. 456-57. "The information which led to the discovery of the conspiracy and its nature and extent was largely obtained by intercepting messages on the telephones of the conspirators by four federal prohibition officers. Small wires were inserted along the ordinary telephone wires from the residences of four of the petitioners and those leading from the chief office. The insertions were made without trespass upon any property of the defendants."

[307] *Id.* at 464.

In *Olmstead*, after he reviewed earlier Supreme Court Fourth Amendment decisions,[308] Chief Justice Taft framed the question regarding Fourth Amendment privacy rights as whether the government had the right to enter private property in order to seize information to be used as evidence without providing due process.[309] Telephones presented a challenge to such a conceptualization because there was no tangible evidence to be obtained.

Chief Justice Justice Taft then referred back to the 1877 case *Ex Parte Jackson*,[310] a case that concerned the government's authority to open and search letters or parcels traveling through the mails. This scenario was analogous to the interception of a phone call being transmitted by a third party. In *Jackson*, Justice Stephen Field wrote, "Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles."[311] In *Olmstead* Justice Taft was given the opportunity to apply the *Jackson* holding to information transmitted electronically. He did not take advantage of the opportunity.

Instead, Taft wrote, "The United States takes no such care of telegraph or telephone messages as of mailed sealed letters."[312] When considering the procedure used

---

[308] *Weeks*, 232 U.S. 383; Silverthorne Lumber Co. v. United States, 251 U. S. 385 (1920); Amos v. United States, 255 U. S. 313 (1921); *and* Gouled v. United States, 255 U. S. 298 (1921).

[309] *Olmstead*, 277 U.S. at 466. He concluded, "Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant, unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure."

[310] 96 U.S. 727 (1877).

[311] *Id.* at 733.

[312] *Olmstead*, 277 U.S. at 464.

by the government to gather the evidence in *Olmstead*, Taft reasoned: "The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."[313] As a result, after *Olmstead,* Fourth Amendment privacy protections attached only to specific spaces.[314] In his dissenting opinion, Justice Brandeis argued thatthe use of technologies that enabled the government to "listen in" to what was transpiring within private space was constitutional, as long as government agents did not bodily enter the space without a warrant.[315] He reasoned: "The language of the amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening

---

[313] *Id.*

[314] *C.f. Id.* at 487 (Butler, J., dissenting). Justice Pierce Butler used a contract analogy to refute third-party doctrine reasoning. He wrote: "Telephones are used generally for transmission of messages concerning official, social, business and personal affairs including communications that are private and privileged those between physician and patient, lawyer and client, parent and child, husband and wife. The contracts between telephone companies and users contemplate the private use of the facilities employed in the service. The communications belong to the parties between whom they pass. During their transmission the exclusive use of the wire belongs to the persons served by it. Wire tapping involves interference with the wire while being used. Tapping the wires and listening in by the officers literally constituted a search for evidence. As the communications passed, they were heard and taken down."

[315] *Id.* at 473 (Brandeis, J., dissenting). In a strong dissent, Justice Brandeis argued that interpretations of constitutional protections would need to be broadened to include new technologies the Founders could not foresee. He warned, "Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." *Id.* Justice Brandeis continued: "Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions." *Id.* at 475 76. Brandeis addressed the specific privacy threat posed by wiretapping when he wrote: "The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping."

wires are not part of his house or office, any more than are the highways along which they are stretched."[316]

In the *Olmstead* decision, Chief Justice Taft implicitly invoked the privacy-as-space conceptualization. He explained: "The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment."[317] Stated, another way, telephonic technology projects personal information, via wire, into public space even though the information might originate within the intimacy of one's own home. One can not reasonably expect information projected outside of the private sanctuary of the home to remain private. This language shaped Fourth Amendment privacy law for the next thirty-two years, and the Court's Fourth Amendment privacy analysis centered upon a determination of whether and under what conditions private space was intruded upon by the government without due process and whether different methods of seizing information required due process.

Ultimately, *Olmstead* was about the utilization of a new surveillance technology, wire tapping, and how that technology infringed upon private space. In 1942 the reasoning in the *Olmstead* decision was used to decide *Goldman v. United States.*[318] In *Goldman*, law enforcement officers attached a device called a "detectaphone" to the wall adjacent to an apartment in which suspects were making phone calls. As with wire

[316] *Id.* at 465.

[317] *Id.* at 466.

[318] 316 U.S. 129 (1942).

tapping in *Olmstead*, officers were able to intercept and "listen" to conversations within the apartment -- a private space -- without entering.

In *Goldman* officers had first entered the apartment, without a warrant, in order to install a listening apparatus. That device failed, and it was only then the officers decided to use the detectaphone, which generated the only information entered into evidence. The Court used the reasoning applied in *Olmstead*. Had the defendant challenged evidence collected by the original bug, the information collected would likely have been ruled inadmissible under the exclusionary rule for violating the Fourth Amendment. Yet, the evidence obtained was admissible because it had been gathered by a device that did not require prior trespass and therefore did not require a warrant. The Court's analysis implicitly protected an individual privacy interest in a private space rather than in the information that was intercepted and recorded.

Conversely, this same logic led to the exclusion of evidence obtained through the government's use of another new listening technology. In *Silverman v. United States*,[319] the Court determined that the use of a "spike mike" without a warrant constituted an unreasonable search. Police officers attached an electronic device—the spike mike—to the heating ducts of a house used by defendants. This device was capable of reading small acoustic vibrations and effectively transformed the home's ductwork into a gigantic microphone running throughout an entire residence. Justice Potter Stewart wrote for the Court and held that the spike mike infringed upon the defendant's Fourth Amendment rights. He also ruled that the evidence so collected was inadmissible because law enforcement officers had entered the basement in order to attach the mike. Under the

[319] 365 U.S. 505 (1960).

Court's Fourth Amendment privacy doctrine, which implicitly applied a spatial privacy conceptualization, such trespass requires a warrant in order to fulfill due process requirements.

Justice Stewart explicitly reinforced the Court's conceptualization of privacy as space when in *Silverman* he refuted the argument that a "re-examination" of the rationale used to decide O*lmstead* and subsequent cases was "essential in the light of recent and projected developments in the science of electronics."[320] He avoided an analysis of the technical capabilities of spike mikes and instead linked the use of the spike mike to a physical invasion of a constitutionally protected private space. Justice Stewart wrote: "[A] fair reading of the record in this case shows that the eavesdropping was accomplished by means of an unauthorized physical penetration into the premises occupied by the petitioners."[321] This language brought *Silverman* in line with *Olmstead* and *Goldman*, and Justice Stewart explicitly stressed that his decision was "based upon the reality of an actual intrusion into a constitutionally protected area."[322] Nevertheless, Justice Stewart was careful to qualify his holding and explain that not all eavesdropping practices involving a physical incursion into private space were subject to due process requirements.

One such exception to the due process requirement involves consent. There are instances when a law enforcement officer is in a private space with permission. For instance, in *On Lee v. United States*, [323] the Court ruled that consent negates the Fourth

[320] *Id.* at 508.

[321] *Id*. at 509.

[322] *Id.* at 512.

[323] 343 U.S. 747 (1952).

Amendment warrant requirement. Justice Robert H. Jackson considered the admissibility of evidence obtained when an undercover agent, who was trusted by the defendant, entered the defendant's laundromat and used a hidden microphone to transmit an incriminating conversation (initiated by the agent) to another agent outside the premises. He held that the transmission had not been obtained by a warrantless search or seizure and was therefore admissible.

Since the informant entered the property with consent, the Court did not determine that the evidence had been gained by trespass or, stated another way, through an invasion of privacy. In *Silverman*, when agents surreptitiously entered the basement of the home for the purpose of attaching the spike mike to the ductwork, they did so without consent and without due process, and their search was thus unreasonable. Eavesdropping became an unreasonable search when conducted in an unauthorized manner, and authorization could be either a warrant or an owner's consent.[324]

In 1966 the Court recognized an additional category of authorized searches. If evidence will disappear unless collected immediately, the Court has permitted law enforcement officers to perform "emergency" collections. In *Schmerber v. California*,[325] a person injured in a car accident was taken to a hospital. A police officer investigating the accident had reason to believe the individual had been driving under the influence of alcohol, so he ordered medical personnel to draw blood and conduct a blood-alcohol test.

---

[324] *Silverman*, 365 U.S. at 510. Justice Potter wrote: "But in both *Goldman* and *On Lee* the Court took pains explicitly to point out that the eavesdropping had not been accomplished by means of an unauthorized physical encroachment within a constitutionally protected area."

[325] 384 U.S. 757 (1966).

Justice Harry Blackmun wrote the opinion of the Court in *Schmerber* and, relying on *Olmstead*, held that information revealed in the blood test, which was given over the objection of the defendant, was admissible. Justice Blackmun noted that because the Court was dealing with "intrusions into the human body rather than with state interferences with property relationships or private papers -- houses, papers, and effects -- we write on a clean slate."[326] He wrote, "The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."[327] This language likened the human body, especially subsurface, to private space. Justice Blackmun wrote, "Search warrants are ordinarily required for searches of dwellings, and absent an emergency, no less could be required where intrusions into the human body are concerned."[328]

Thus, Justice Blackmun had established that the body was a variant of private space, and he then focused on whether the blood test was an unwarranted intrusion into that space. He first determined that the officer had probable cause to suspect a crime had been committed. Justice Blackmun wrote: "The police officer who arrived at the scene shortly after the accident smelled liquor on petitioner's breath, and testified that petitioner's eyes were 'bloodshot, watery, sort of a glassy appearance.' The officer saw petitioner again at the hospital, within two hours of the accident. There he noticed similar symptoms of drunkenness."[329] Justice Blackmun accepted these observations as a valid showing of cause, and then the analysis turned to the question of due process. The Court

[326] *Id.* at 767-68.

[327] *Id.* at 767.

[328] *Id.* at 770.

[329] *Id.* at 768-69.

needed to determine if there was a justification for the officer electing to forgo the warrant process prior to ordering the blood test.

After reviewing testimony from the lower courts, Justice Blackmun reasoned that the blood test was not an unreasonable Fourth Amendment search because the officer "might reasonably have believed that he was confronted with an emergency, in which the delay necessary to obtain a warrant, under the circumstances, threatened the destruction of evidence."[330] He likened such a search to an officer checking a suspect for concealed weapons—evidence of a crime—immediately after an arrest. In *Schmerber* there was a real chance that the officer's evidence would quite literally disappear unless there was an immediate search. Justice Blackmun noted: "We are told that the percentage of alcohol in the blood begins to diminish shortly after drinking stops, as the body functions to eliminate it from the system. Particularly in a case such as this, where time had to be taken to bring the accused to a hospital and to investigate the scene of the accident, there was no time to seek out a magistrate and secure a warrant."[331] Thus under the privacy-as-space conceptualization, the Court had established two exceptions to due process requirement: consent and emergency circumstances.

In sum, the 1928 *Olmstead* decision separated Fourth Amendment analysis from Fifth Amendment analysis and solidified the privacy-as-space conceptualization within Fourth Amendment doctrine. The Court has limited its review to the question of whether an invasion of constitutionally protected space had occurred. There were three conditions under which the Court ruled that it is reasonable to access information from within such

[330] *Schmerber*, 384 U.S. at 770.

[331] *Id.* at 770-71.

space. First, law enforcement may do so with judicial oversight. Such oversight is confirmed through the warrant process. Second, if the defendant granted consent to law enforcement officers to enter his or her private space, those officers can use any information they access, even if they are acting undercover or transmitting the information to a third party off the premises. Lastly, it is reasonable for evidence to be collected without a warrant if special circumstances exist making it impossible for law enforcement to comply with due process requirements and still access vital evidence. This was the Court's approach to Fourth Amendment privacy until a landmark 1967 decision—dealing with portable technology that allowed law enforcement officers to eavesdrop on individuals outside of their home—in which the Court decided that the Fourth Amendment protected people and not just places.

Privacy as Secrecy

In 1967 Justice Potter Stewart wrote for the Court and overturned *Olmstead* in *Katz v. United States*.[332] In *Katz* the Court embraced a new conceptualization of Fourth Amendment privacy, privacy as secrecy. Instead of focusing on the government's intrusion into a specific private space, analysis focused on whether an individual had created and was thereby entitled to a reasonable expectation of privacy.

As discussed in Chapter 1, the privacy-as-secrecy conceptualization treats privacy as a commodity. One surrenders all of a particular privacy interest (for instance in medical information) when he or she surrenders any one part of it to another individual (doctor). Privacy as secrecy does not embrace the notion of limited privacy and instead is

[332] 389 U.S. 347 (1967).

predicated upon the third-party doctrine. Later, at the opening of the twenty-first century, the Court would start to embrace limited privacy in Fourth Amendment jurisprudence. Until that time, only information purposely not shared with third parties could be considered private.

Charles Katz, the appellant, was convicted of violating a federal statute prohibiting the use of a "wire communication facility for the transmission in interstate or foreign commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest."[333] Katz had made gambling calls from a public phone booth. Law enforcement officers used a listening device attached to the outside of the telephone booth to access and record his side of the conversations. Katz was convicted with the evidence they gathered.

Katz argued that bugging the telephone booth infringed upon his Fourth Amendment protections against an unreasonable search and seizure. Utilizing the reasoning in *Olmstead*, the government argued that since there was no physical invasion of the phone booth, there was no Fourth Amendment violation. The government also asserted that a telephone booth was public, that individuals using the phone could be seen by anyone, and that it was not a constitutionally protected space.

Justice Stewart rejected *Olmstead* and explicitly moved the Court beyond the privacy-as-space conceptualization. He reconceptualized individual privacy interests under the Fourth Amendment as protecting an individual right to conceal certain information and materials rather than physical space. Justice Stewart outlined this transformation when he wrote:

---

[333] 18 U.S.C. § 1084(a).

> [T]he effort to decide whether or not a given "area," viewed in the abstract, is "constitutionally protected" deflects attention from the problem. . . . For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.[334]

With these words, Fourth Amendment privacy protections were defined by personal agency, actions taken by individuals to create a subjective expectation of privacy. After *Katz*, Fourth Amendment analysis would largely focus on the question of whether society at large would consider the plaintiff's self-defined expectation of privacy to be reasonable. Generally, the only information that might be constitutionally protected was that "knowingly" concealed by individuals. The third-party doctrine now became a core component of privacy in Fourth Amendment privacy cases. Information shared with a third party was no longer protected under the Fourth Amendment.

In *Katz*, Justice Harlan wrote a famous concurrence in which he stated, "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[335] This became the new test for Fourth Amendment privacy invasion and, as mentioned above, it made personal agency central to defining constitutionally protected privacy. Since *Katz*, the Court has reviewed individual efforts to create a subjective expectation of privacy.

For instance, in K*atz* Justice Harlan wrote:

---

[334] *Katz*, 389 U.S. at 350-51.

[335] *Id.* at 361 (Harlan, J., concurring).

> The critical fact in this case is that (o)ne who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to "assume" that his conversation is not being intercepted. The point is not that the booth is "accessible to the public" at other times, but that it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable.[336]

Here personal agency was recognized in the act of closing the phone booth door and paying the phone company for a private line. The Court held that Katz had taken sufficient actions to create a zone of privacy.

Justice Hugo Black wrote a dissenting opinion in *Katz* in response to the Court's "rewriting of the Fourth Amendment" and warned that after *Katz* the Amendment would no longer be interpreted as protecting citizens solely against "unreasonable searches and seizures," but rather as protecting the broader notion of every "individual's privacy."[337] Justice Black feared that the broad expansion of Fourth Amendment protections might render it useless. He noted: "Few things happen to an individual that do not affect his privacy in one way or another. Thus . . . the Court has made the Fourth Amendment its vehicle for holding all laws violative of the Constitution which offend the Court's broadest concept of privacy."[338]

Justice Stewart did acknowledge the need to limit the scope of Fourth Amendment protections. Though he believed "the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area,'" Justice Stewart qualified this expansion by holding that "the Fourth

---

[336] *Id.*

[337] *Id.* at 373 (Black, J., dissenting).

[338] *Id.*

Amendment cannot be translated into a general constitutional right to privacy."[339] Moreover, the third-party doctrine itself actually limits the scope of protected information since modern life often compels individuals to share information with third parties in return for services.

Justice Stewart held that each individual had a "general right to privacy," which was conceptualized as "his right to be let alone by other people," but he did not recognize this general right as a fundamental constitutional right but instead "like the protection of his property and of his very life [to be] left largely to the law of the individual States."[340] Justice Stewart limited Fourth Amendment privacy to a consideration of the conditions under which the Constitution required due process. Thus, after *Katz*, Fourth Amendment privacy was not a fundamental right to be left alone, but rather a right of individuals to compel government to provide due process prior to accessing "what [an individual] seeks to preserve as private, even in an area accessible to the public."[341]

Again, implicit in this distinction between what privacy interests were protected or unprotected is the notion of personal agency. An individual must have made an effort to preserve something as private if he or she wants to invoke constitutional protection. Thus, even as it embraced the privacy-as-secrecy conceptualization, the Court necessarily framed a concurrent privacy right as the right to control access to information. In *Katz* Justice Stewart recognized Katz's effort to keep his conversation private when he held that because "a person in a telephone booth . . . shuts the door behind him, and pays the

[339] *Id.* at 350.

[340] *Id.* at 350-51.

[341] *Id.*

toll . . . [he] is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[342] Were the door left open, the privacy interest would be lost.

Justice Stewart noted that the Court had "departed from the narrow view on which [the *Olmstead*] decision rested."[343] He wrote:

> [T]he Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements overheard without any [trespass] . . . . Once this much is acknowledged, and once it is recognized that the Fourth Amendment protects people--and not simply "areas"--against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.[344]

The Court held that under this new conceptualization of Fourth Amendment privacy, "[t]he fact that the electronic device employed . . . did not happen to penetrate the wall of the booth can have no constitutional significance."[345] Justice Stewart stressed this portable aspect of personal agency under the Fourth Amendment when he explained: "These considerations do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth. Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[346] Fourth Amendment privacy protections henceforth attached to individuals.

---

[342] *Id.* at 352.

[343] *Id.* at 353.

[344] *Id.*

[345] *Id.*

[346] *Id.* at 359. *See also* Terry v. Ohio, 392 U.S. 1, 89 (1968) (explaining, in a case examining a confrontation in a street between a police officer and a citizen, that this right of privacy attaches "as much to the citizen on the streets of our cities as to the homeowner closeted in his study to dispose of his secret affairs").

Fourth Amendment analysis therefore needed to determine in which contexts an individual could claim Fourth Amendment protections. It was the concurring opinion of Justice John M. Harlan in *Katz* that created the two-part test that is still used today. In order to invoke constitutional protection against unreasonable searches and seizures, individuals must demonstrate in court that they knowingly created a condition under which they believed particular information or material would remain private, their subjective expectation of privacy. Once this personal agency had been established, they would then need to convince the court that their expectation of privacy was reasonable according to societal standards. This two-part test has been applied to Fourth Amendment privacy cases since *Katz.*[347]

For instance, in *Smith v. Maryland*[348] the Court applied the *Katz* test in a case involving the use of yet another technology used to monitor phone calls, the pen register. These are devices that phone companies routinely use to record the phone numbers dialed from a particular phone. This technology is primarily used to record for billing purposes how many long distance calls a particular customer makes during a particular billing period. In *Smith*, law enforcement officers used a pen register to establish that their suspect was making harassing phone calls to the victim of a prior crime.

---

[347] The Court has not retroactively applied the two-part test from *Katz* to alleged infringements that might have taken place prior to 1967. *See* United States v. White, 401 U.S. 745, 754 (1971) (The Court ruled on a case involving an informant who wore a wire when he conversed with a suspect in a number of locations in 1965 and 1966 including the suspect's home. The Court held that *On Lee* was still binding precedent when it held: "It was error for the Court of Appeals to dispose of this case based on its understanding of the principles announced in the *Katz* case. The court should have judged this case by the pre-*Katz* law and under that law, as *On Lee* clearly holds, the electronic surveillance here involved did not violate White's rights to be free from unreasonable searches and seizures." The decision in *White* turned once again on the fact that there was no physical trespass involved in gathering the information and that the suspect willingly conversed with the informant.)

[348] 442 U.S. 735 (1979).

During a robbery, alleged thief Michael Lee Smith acquired the home phone number and address of his victim, Patricia McDonough. For weeks after the robbery he made threatening phone calls to her home and even drove by her home to terrorize her. The police had a physical description of Smith and his car that was provided by McDonough. When police spotted a man who looked like Smith they recorded his license plate number and thereby learned his home address. In an effort to determine if it was indeed Smith making the harassing calls to McDonough, police asked the phone company to attach a pen register device to his home phone. It did, and this information ultimately led to his arrest. Smith claimed that the use of the pen register technology without a warrant was an unreasonable search and seizure.

In *Smith*, Justice Harry A. Blackmun held that the use of the pen register by the phone company did not rise to the level of a "search" within the meaning of the Fourth Amendment because Smith had willingly shared the phone numbers he wanted to dial with a third party, the phone company. Justice Blackmun wrote, "Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner obviously cannot claim that his 'property' was invaded or that police intruded into a 'constitutionally protected area.'"[349] Instead, using *Katz*, the Court considered whether Smith had a subjective expectation of privacy in the phone numbers he dialed into his phone.

[349] *Id.* at 741. One important distinction between *Smith* and *Katz* is that pen registers cannot record any of the content of the communication transpiring on the phone lines as the "bug" in *Katz* could. The pen register records only digits that necessarily have to be shared with the phone company in order to complete a call; *But see. Id.* at 748 (Stewart, J., dissenting) (arguing that the numbers dialed from a private telephone "are not without content" and that a list of numbers might easily reveal the identities of the persons and the places called and thus reveal the most intimate details of a person's life).

The basis of Justice Blackmun's decision in *Smith* was the third-party doctrine upon which the privacy-as-secrecy conceptualization is predicated. He determined that society in general would not consider "any actual expectation of privacy in the numbers they dial" to be reasonable, and he stressed that individuals choose to trade knowledge of the numbers they dial for phone service.[350] He wrote, "All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[351]

This brought the idea of personal agency into the analysis. Smith traded some of his privacy for the convenience of phone service. If he strongly desired to keep his communication private, he might have forgone the telephone in favor of sending letters by post. Justice Blackmun reasoned that phone subscribers expect the phone company to track whom they call. He noted, "All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills."[352] Thus, absent any action on Smith's part to conceal the phone numbers he dialed and in light of the fact that he shared the information willingly with a third party, Justice Blackmun found that when the police used the pen register device to identify Smith as the individual making the calls, they did not commit an unreasonable search or seizure. Smith's conviction was upheld.

In a dissenting opinion that foreshadowed a direction the Court would eventually take in its Fourth Amendment doctrine, Justice Thurgood Marshall argued: "Privacy is

---

[350] *Id.* at 742.

[351] *Id.*

[352] *Id.*

not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[353] Justice Marshall argued for the right to limited privacy to enable individuals to share information with one party and not another.

This notion is at the core of the privacy-as-information-control conceptualization, and Justice Marshall was thus previewing the Court's reconceptualization of privacy under the Fourth Amendment that would occur in 2001. When the Courts eventually did embrace limited privacy, the privacy-as-secrecy conceptualization lost its practical applicability for privacy plaintiffs. The courts would continue, however, to consider the extent to which information had been shared with third parties when determining the appropriate level of constitutional protection a particular type of information derserves.

In 1986 the Court again applied the two-part *Katz* test in order to determine whether individuals might have a reasonable expectation of privacy in those portions of their backyards that can be seen from the air. Chief Justice Warren E. Burger penned the decision in *California v. Ciraolo*[354] in which the petitioner appealed his conviction for growing marijuana in his backyard because the government used evidence gathered through aerial surveillance, which the petitioner claimed was an unconstitutional search.

The Court reasoned that anything outside of the home that can be seen from a public space with the naked eye cannot be considered private information. Again, the

---

[353] *Id.* at 749 (Marshall, J., dissenting).

[354] 476 U.S. 207 (1986).

Court relied upon the privacy-as-secrecy paradigm and the third-party doctrine. Anything left in plain sight is being shared with the public and thus cannot be private.

The petitioner in *Ciraolo* claimed that he had built a large fence around his yard for the express purpose of preventing others from being able to see the space from the street. Thus, he argued that he had a legitimate expectation of privacy. Chief Justice Burger agreed that spaces in such close proximity to one's home are generally considered by society to be rather private. He noted, "The protection afforded the curtilage[355] is essentially a protection of families and personal privacy in an area intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened."[356] Nevertheless, when the third-party doctrine was applied to curtilage, the fact that the space could be seen from public areas eroded the privacy interest that attached to such space. Chief Justice Burger wrote: "That the area is within the curtilage does not itself bar all police observation. The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."[357]

Personal agency requirements were heightened in *Ciraolo*. In *Katz*, merely closing the phone booth door and depositing a dime were sufficient to establish a reasonable expectation of privacy. In *Ciraolo* the Court said that building a fence was not sufficient. Chief Justice Burger held that the mere fact "that an individual has taken measures to restrict some views of his activities does not . . . preclude an officer's

---

[355] BLACK'S LAW DICTIONARY 411 (8th ed., 2004). Curtilage is "the land or yard adjoining a house, usually within an enclosure. Under the Fourth Amendment, the curtilage is an area usually protected from warrantless searches."

[356] *Ciraolo*, 476 U.S. at 212-13.

[357] *Id.* at 213.

observations from a public vantage point where he has a right to be and which renders the activities clearly visible."[358]

He did not mention in his decision the extreme measures the police had undertaken to view Ciraolo's property. They had to access an aircraft and fly over. The language used by Chief Justice Burger -- "Any member of the public flying in this airspace who glanced down could have seen everything that these officers observed"[359] -- made it seem as though officers routinely fly overhead and peer into yards! Burger concluded, "The Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye."[360] The decision in *Ciraolo* was in line with the reasoning in *Katz* and *Smith*, and it eroded individual privacy interests even further by elevating the level of personal agency required to create a subjective expectation of privacy by including anyone in the public airspace among third parties sufficient enough to strip away Fourth Amendment protection.

Two years after *Ciraolo*, the Court again expanded the third-party doctrine. In *California v. Greenwood*,[361] the Court said that individuals have no reasonable expectation of privacy in the contents of their garbage bags once trash has been placed at the curb for pick-up. In this case, police searched a narcotics suspect's garbage bags for evidence of illegal drug activity, and the evidence gathered was used as probable cause to

---

[358] *Id.*

[359] *Id*. at 213-14.

[360] *Id*. at 215.

[361] 486 U.S. 35 (1988).

get a search warrant, which ultimately led to an arrest. Justice Byron R. White delivered the opinion of the Court, and he based his decision upon the societal standard regarding a reasonable expectation of privacy in garbage. He wrote: "It may well be that respondents did not expect that the contents of their garbage bags would become known to the police or other members of the public. An expectation of privacy does not give rise to Fourth Amendment protection, however, unless society is prepared to accept that expectation as objectively reasonable."[362] Justice White held that society was not.

Using reasoning similar to that in *Smith*, the Court reasoned that the trash is being handed to a third party in return for a service, garbage pick-up. Justice White noted "It is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public." This language invoked the third-party doctrine as the decision explicitly noted that the garbage was removed from the privacy of the home and exposed to the public. Moreover, Justice White wrote, "[R]espondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so."[363]

The Court's adoption of the privacy-as-secrecy conceptualization, predicated upon the third-party doctrine and a personal agency requirement, eroded individual privacy protections under the Fourth Amendment. Up until the *Greenwood* decision, the Court had not explicitly used the notion of limited privacy to limit the effects of the third-

[362] *Id.* at 39-40.

[363] *Id.* at 40.

party doctrine in Fourth Amendment privacy decisions. In 2001 it recognized that new surveillance technologies erode an individual's ability to conceal information, and in a landmark case the Court took an important first step in upholding the primacy of personal agency in constitutional privacy law.

Privacy as Information Control

In *Smith*, Justice Thurgood Marshall had dissented because he felt that intimate information about one's life could be derived from a careful examination of the phone numbers he or she dialed. In *Greenwood*, Justice Brennan wrote a dissent that made the very same point. The contents of a garbage bag could illuminate many facets of someone's life. Receipts, junk mail, food containers, and other types of trash might provide a snapshot of how life is lived within a particular residence.[364]

Ultimately, the basis of Brennan's dissent was that society held a strong expectation of privacy in waste. He argued: "Scrutiny of another's trash is contrary to commonly accepted notions of civilized behavior. I suspect, therefore, that members of our society will be shocked to learn that the Court, the ultimate guarantor of liberty, deems unreasonable our expectation that the aspects of our private lives that are concealed safely in a trash bag will not become public."[365] Thus, Brennan added his voice

[364] *Id.* at 50 (Brennan, J., dissenting). Justice Brennan wrote: "A single bag of trash testifies eloquently to the eating, reading, and recreational habits of the person who produced it. A search of trash, like a search of the bedroom, can relate intimate details about sexual practices, health, and personal hygiene. Like rifling through desk drawers or intercepting phone calls, rummaging through trash can divulge the target's financial and professional status, political affiliations and inclinations, private thoughts, personal relationships, and romantic interests."

[365] *Id.*

to Marshall's in recognizing that the law ought to prohibit access to personal information—whether phone numbers dialed or bits of information discarded in the trash—without a warrant.

The most recent landmark case in the Fourth Amendment privacy doctrine was decided in 2001, and it changed again the way the Court conceptualized privacy.[366] Justice Antonin Scalia wrote the majority decision in *Kyllo v. United States*, which held that the warrantless use of sense-enhancing technology to access information that would otherwise be inaccessible from within a constitutionally protected space was an unreasonable search under the Fourth Amendment. Justice Scalia framed the question decided in the case as "what limits [are there] upon this power of technology to shrink the realm of guaranteed privacy."[367]

Throughout Fourth Amendment jurisprudence, technologies such as wire taps, detectaphones, hidden transmitters, airplanes, and spike mikes had slowly lessened the relevance of physical space to a society's notion of what a reasonable expectation of privacy actually was. Personal agency was also eroded by each succeeding generation of surveillance technology. Most individuals were unaware of the types of listening technologies in use and therefore were unable to take steps to conceal their information, materials, or activities. The Court needed to reconceptualize the privacy interests protected by the Fourth Amendment.

Implicit in the *Kyllo* decision was that the Fourth Amendment really protected the right of individuals to prevent government from accessing information in any

[366] Kyllo v. United States, 533 U.S. 27 (2001).

[367] *Id.* at 34.

circumstance in which new surveillance technologies prevent individuals from being able to create a reasonable expectation of privacy. Thus, in *Kyllo* the Court adopted its fourth conceptualization of privacy under the Fourth Amendment, privacy-as-information-control. In *Boyd* the Amendment protected one from self-incrimination. In *Olmstead* it protected private space. In *Katz* it protected individuals, and then in *Kyllo* it protected information.

In *Kyllo*, the Court reviewed the conviction of Danny Kyllo for growing marijuana in his home. Police used a thermal imager, a camera that records heat waves radiating from within a building.[368] Heat signatures read from one wall of Kyllo's home and from his garage were sufficiently strong to convince police officers that Kyllo was using high intensity lamps to grow marijuana in his home. These heat signatures provided sufficient probable cause to get a warrant to search Kyllo's home, find the plants, and make an arrest. Kyllo later asserted that the use of the thermal imaging equipment was an unreasonable search.

New surveillance technology has made it possible to "search" private spaces—in the sense of being able to discern information regarding what actions, individuals, or objects are within such spaces—with no need for police to approach or enter upon constitutionally protected areas. In *Kyllo,* Justice Scalia implicitly defined privacy as a right to prevent the government from knowing rather than to prevent the government from entering absent due process. In *Kyllo*, the Court defined private spaces not in the context of private property and ownership, but rather in the language from *Katz.* Private

[368] Agents used an Agema Thermovision 210 thermal imager to scan Kyllo's triplex.

spaces were those in which, historically, individuals had enjoyed an expectation of privacy that society in general would consider reasonable.

If the use of surveillance technology that eliminates the need to enter a private space were enough to qualify a search as reasonable, then the Court's analysis would be purely mechanical. The Court need only establish that law enforcement officials were in a public space when using the technology. In *Kyllo*, Justice Scalia wrote, "We rejected such a mechanical interpretation of the Fourth Amendment in *Katz,* where the eavesdropping device picked up only sound waves that reached the exterior of the phone booth."[369] The apparatus being used in *Kyllo* read heat waves emanating from the walls of the home rather than sound waves, but the idea was generally the same. Adhering to the Court's reasoning in *Katz*, Scalia argued, "Reversing that approach would leave the homeowner at the mercy of advancing technology--including imaging technology that could discern all human activity in the home."[370]

Thus, *Kyllo* established that it is not the square footage of a space that was protected, but rather government access to knowledge of what transpires within that private space. Justice Scalia wrote:

> We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' . . . constitutes a search--at least where (as here) the technology in question is not in general public use.[371]

[369] *Kyllo*, 533 U.S. at 35-36.

[370] *Id.*

[371] *Id.* at 34.

This language brings *Kyllo* in line with *Silverman* and *Katz* and implies that the Fourth Amendment has always been about accessing information, not invading space.

The earlier Fourth Amendment cases discussed above dealt with familiar technologies or technologies that required physical access to a home. If individuals are familiar with a given technology, they will understand the steps they need to take to create a reasonable expectation of privacy. For instance, binoculars and telescopes enhance one's sense of sight. In adjacent high-rise buildings in big cities, individuals know they can easily be watched through their windows by others using these technologies. They also understand how to foil these "peeping toms" by drawing their shades.

In *Ciraolo*, marijuana plants were seen from the public airspace with the naked eye. Had the thought occurred to him, Ciraolo could have taken steps to conceal the plants from observation from the sky with mesh netting or tarps. In *Katz* the petitioner had taken the precautions necessary to conceal his conversation by closing the phone booth door, yet technology was still able to invade that private space. The Court in *Katz* said that use of the listening technology was unconstitutional because Katz had taken reasonable steps to maintain an expectation of privacy and could not reasonably be expected to take further steps to foil a small transmitter placed on the outside of the phone booth.

In *Kyllo* the police used technology that was rather rare, and it would not normally occur to citizens that the inside of their homes could be monitored in such a way. After considering societal awareness of new technologies, Justice Scalia used the Fourth Amendment privacy jurisprudence to reinforce personal agency in circumstances

in which new technologies inhibit the ability of individuals to define a subjective expectation of privacy. He also emphasized the sanctity of the home as a constitutionally protected space. Justice Scalia assigned a more substantial individual privacy interest whenever an invasion of the home is involved. He wrote: "These were intimate details because they were details of the home, just as was the detail of how warm--or even how relatively warm--Kyllo was heating his residence."[372] Thus access to information about what is transpiring within intimate spaces warrants additional protection. In hisopinion , Justice Scalia quoted *Payton v. New York* when he reaffirmed that "the Fourth Amendment draws a firm line at the entrance to the house,"[373] and then wrote, "That line, we think, must be not only firm but also bright--which requires clear specification of those methods of surveillance that require a warrant."[374]

After he reemphasized that the home is a constitutionally protected area, Justice Scalia then reinforced the role of personal agency. He seized the notion of familiarity as a standard for determining when the use of a particular technology would require a warrant. If a technology was generally familiar to the public, like binoculars, then individuals must create a subjective expectation of privacy by taking some action, like drawing the blinds. However, Justice Scalia wrote, "Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is

[372] *Id.* at 38.

[373] 445 U.S. 573, 590 (1980).

[374] *Kyllo*, 533 U.S. at 40.

presumptively unreasonable without a warrant."[375] Here the Fourth Amendment had evened the playing field.

Privacy under the Fourth Amendment

Within Fourth Amendment privacy doctrine, the Court's conceptualization of privacy has evolved through four distinct stages: Fourth and Fifth Amendment due process, privacy as space, privacy as secrecy, and privacy as information control. Originally, Fourth Amendment protections were enmeshed with the Fifth Amendment's protection against self-incrimination. The Fourth Amendment was directly inspired by the English government's use of writs of assistance and general warrants prior to the American Revolution and the founders' concern over government intrusions upon private property for the purpose of obtaining material evidence to be used against individuals in court. Thus during the first stage of Fourth Amendment jurisprudence, the court generally combined Fourth and Fifth Amendment interests as was typified in *Boyd*.

The Court then established Fourth Amendment analysis as being distinct from Fifth Amendment analysis. Starting with *Olmstead,* the Court conceptualized privacy as a right to protect private space. Court decisions under the privacy-as-space conceptualization generally involved guaranteeing that the government procured a warrant prior to invading any private space absent consent or emergency, evidentiary concerns.

Then in *Katz*, the Court implicitly reconceptualized privacy as secrecy. During this period the Court would determine whether an individual had taken sufficient action

[375] *Id.*

to create a subjective expectation of privacy in certain information, materials, or space. Once such personal agency had been established, the Court would determine whether that subjective expectation of privacy was one that society in general would recognize as reasonable. The privacy-as-secrecy conceptualization was predicated upon the third-party doctrine. The notion of limited privacy was not considered by the Court during this stage, so information that was shared with a third party could no longer be considered private in a constitutional sense.

The final and nascent conceptualization of privacy that has been recognized by the Court is privacy as information control. In *Kyllo* the Court recognized that new surveillance technologies were eroding the significance of historically private spaces, such as one's home, along with protection provided by personal agency in Fourth Amendment privacy decisions. In response, the Court explicitly recognized a heightened privacy interest in private homes and in situations wherein the government uses surveillance technology that is generally unfamiliar to the public. In *Kyllo* the Court implicitly held that the Fourth Amendment does not protect space so much as it protects government knowledge of what transpires within a particular space. Thus, the advent of new surveillance technologies has caused the Court to conceptualize privacy as an individual's right to control access to information in Fourth Amendment privacy jurisprudence.

CHAPTER IV

CONFIDENTIALITY IN INFORMATION PRIVACY CASES

The review of First and Fourth Amendment privacy jurisprudence provided in Chapters 2 and 3 revealed a gradual process through which the U.S. Supreme Court's conceptualization of a constitutional right to privacy has become increasingly about an individual's right to control access to, manipulation of, and dissemination of personal information. The older privacy-as-space and privacy-as-secrecy conceptualizations used by the Court in these doctrines were eventually reinterpreted and described in terms of a right to manipulate information flow. Thus, the privacy-as-information control conceptualization of privacy will likely inform the legal analysis in any future constitutional challenges to KDD dataveillance on privacy grounds.

In 1977 the Supreme Court recognized a distinct right of individuals to "avoid the disclosure of personal matters."[376] This established a new privacy doctrine, information privacy, which protects individuals against the government's ability to learn about personal aspects of their lives by accessing and analyzing their personal information. Since KDD technologies enable the government to obtain such personal insights with unprecedented ease, understanding how the courts conceptualize privacy in information privacy cases is necessary to an evaluation of the strength of constitutional privacy protections against KDD dataveillance. The following examination of information

[376] Whalen v. Roe, 429 U.S. 589, 600 (1977).

privacy cases in which statutes or officials have compelled individuals to surrender control of their personal information to the government reveals the emergence of a new conceptualization of privacy, privacy as confidentiality.

In information privacy law, the privacy-as-information-control conceptualization has already partly evolved into a privacy-as-confidentiality conceptualization. The difference between the two lies with the agent of control. In the first, individuals retain control over their own information. For example, in the pamphleteer cases in Chapter 2, the Courts consistently held that individuals rather than the state should control when to disclose their identifying information and to whom. In the second, individuals hold the government to a "duty" of confidentiality absent a substantial or compelling government interest to justify disclosure. In information privacy cases, this duty typically is considered fulfilled if the government can demonstrate the implementation of either statutory or procedural safeguards designed to protect against the unnecessary dissemination of personal information that has been surrendered to the government. The level of protection required of these safeguards varies depending upon the nature of the information under consideration.

Though information privacy law has been described as "a mosaic of various types of law,"[377] this chapter is concerned only with constitutional information privacy and begins with a review of the two Supreme Court cases credited with creating a distinct privacy right in personal information and a third that is widely cited by the circuit courts regarding which types of information are entitled to protection. Then decisions from the circuit courts are discussed in order to define the current scope of the privacy interest in

[377] SOLOVE, *supra* note 4, at 56.

avoiding the disclosure of personal matters in general and the courts' recognition of privacy-as-confidentiality conceptualization in particular. Each appellate case was selected because it discussed the constitutional privacy right first framed by the U.S. Supreme Court's dicta in *Whalen v. Roe*,[378] the individual privacy interest in "avoiding disclosure of personal matters."[379]

Information Privacy and the Supreme Court

As previously discussed, the dicta in *Whalen v. Roe*[380] distinguished between privacy interests involving independence in making personal decisions and privacy interests in personal information for the first time. Moreover, when Justice John Paul Stevens wrote, "The right to collect and use [data] for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures . . . . [I]n some circumstances that duty arguably has its roots in the Constitution . . . ,"[381] he explicitly recognized a new conceptualization of privacy, privacy as confidentiality. Since *Whalen*, the courts have been gradually shaping this right to confidentiality in personal information surrendered by individuals to the government.

Whalen involved a challenge to a New York statute[382] that required physicians to

---

[378] 429 U.S. 589 (1977).

[379] *Id.* at 598-600.

[380] 429 U.S. 589 (1977).

[381] *Id.* at 605.

[382] New York State Controlled Substances Act of 1972, N.Y.LAWS, 878, N.Y.PUB.HEALTH LAW § 3300 (McKinney, Supp. 1976-1977). The statute attempted to limit the distribution of drugs that have both legitimate and illegitimate uses.

submit to the New York State Health Department personal information[383] for patients receiving prescriptions for a number of addictive drugs.[384] The health department would then store these data on computer tapes, and law enforcement could access and use the data to identify patients and physicians who might be abusing or defrauding prescription plans for the purpose of obtaining the addictive drugs.

The patients and physicians who filed the suit argued that the statute constituted an invasion of privacy. Their central contention was that individuals requiring these medications might not fill prescriptions for fear that "misuse of the computerized data" might result in their social "stigmatization" as "drug addicts."[385] The district court had found that the statute unnecessarily intruded upon the "doctor-patient relationship," which was considered to be one of the "zones of privacy afforded constitutional protection."[386]

Writing for the Court, Justice John Paul Stevens noted: "The cases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[387]

---

[383] Whalen v. Roe, 429 U.S. 589, 593 (1977). Information collected included "prescribing physician; the dispensing pharmacy; the drug and dosage; and the name, address, and age of the patient."

[384] *Id.* at 593, n.8 (1977). This footnote identified "Schedule II" drugs that were targeted by this statute as "opium and opium derivatives, cocaine, methadone, amphetamines, and methaqualone" and explained that "these drugs have accepted uses in the amelioration of pain and in the treatment of epilepsy, narcolepsy, hyperkinesia, schizo-affective disorders, and migraine headaches."

[385] *Id.* at 595. At trial, plaintiffs entered into evidence the stories of a number of individuals who declined treatment and of doctors who would no linger prescribe the medications. *Id.*, at n. 16.

[386] Roe v. Ingraham, 403 F.Supp. 931 (D.C.N.Y. 1975).

[387] *Whalen*, 429 U.S. at 598-600.

His recognition of an interest in avoiding disclosure of personal matters was the beginning of a new privacy doctrine, information privacy, but *Whalen* provided little insight into the constitutional roots of this new strand of privacy other than holding that it existed in the penumbras of specific protections in the Bill of Rights as established in *Griswold v. Connecticut*[388] and that it was a "personal liberty" protected from violation by the states by the Fourteenth Amendment as established in *Roe v. Wade*.[389] Justice Stevens accepted the argument that information could leak and said that fear that their use of these drugs might become publicly known could make "some patients reluctant to use, and some doctors reluctant to prescribe, such drugs even when their use is medically indicated."[390] Thus, Justice Stevens recognized that the New York statute "threatens to impair both [patients'] interest in the nondisclosure of private information and also their interest in making important decisions independently."[391]

Since Justice Stevens held that the privacy interests threatened in *Whalen* were protected liberties under the Fourteenth Amendment, the Court would apply substantive due process review in the case. This standard of review generally involves balancing the content of a regulation and the governmental interest in regulating an activity against the individual privacy interest that is being infringed upon by the legislation. In *Whalen*, the government's interest was in preventing prescription drug fraud while the privacy interest was the possibility that those who needed these medications would refrain from using

---

[388] 318 U.S. 479 (1965).

[389] 410 U.S. 113, 152 (1973).

[390] *Whalen*, 429 U.S. at 600.

[391] *Id.*

them. In other words, the patient's usage behavior or the doctor's prescribing behavior might be chilled.

Justice Stevens considered the content of the statute and whether evidence of a behavioral chill existed. In particular, he focused on safeguards within the statute designed to protect personal information surrendered to the state. He held, "The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures."[392] New York State argued that the statute provided adequate procedural safeguards to protect the personal information both when it was initially submitted on paper forms as well as after the information was transcribed onto computer tape.[393]

Though he noted that information leaks might still occur despite the provisions, Justice Stevens ultimately upheld the New York statute because its duty to safeguard the patient information had been fulfilled by what he regarded as adequate safeguards for information handling within the statute.[394] It is this expectation of the fulfillment of a "concomitant duty" that comprises the core of the privacy-as-confidentiality conceptualization. Individuals have a right to expect that the government will keep

---

[392] *Id.* at 605.

[393] *Id.* at 594. The statutory safeguards included the fact that following transcription, the remaining paper forms were stored in a vault for five years before being destroyed; the receiving room is surrounded by a locked wire fence and protected by an alarm system; and once the information was on magnetic tape, the statute provided that the tapes were "kept in a locked cabinet. . . . When the tapes are used, the computer is run 'off-line,' which means that no terminal outside of the computer room can read or record any information;" and, regarding the personnel responsible for transcribing and archiving the information, the statute mandated, "Public disclosure of the identity of patients is expressly prohibited by the statute and by a Department of Health regulation."

[394] *Id.* at 595. Justice Stevens held that the mere possibility that security leaks might occur or that personal information might be disclosed as evidence at trial was not sufficient to invalidate the statute on its face.

confidential the personal information it compels them to disclose, absent a legitimate state interest.

After he accepted the statutory safeguards, Justice Stevens considered whether the infringement upon information privacy rights might cause a behavioral chill. He relied upon drug-use statistics supplied by the state health department and compared the usage rates of those medications regulated by the statute before and after it was enacted. After completing the comparison, the Court held that "the statute did not deprive the public of access to the drugs."[395] Justice Stevens distinguished *Whalen* from decisional privacy cases involving statutes that banned particular choices altogether. He summarized three types of state interference in an individual's ability to make intimate decisions: outright bans on specific behaviors (laws against abortions, assisted suicide, etc.); state licensing of particular behaviors (you need permission from the state to hunt, drive, sell liquor, etc.); and state collection of information regarding individuals choosing to take specific actions. The New York statute fit in the last category.[396]

Justice Stevens concluded that the statute does not insert the state directly into the doctor-patient relationship because "access to these drugs [is not] conditioned on the consent of any state official or other third party."[397] Having established a legitimate purpose for the statute, adequate information safeguards, and that the state was not "chilling" behavior regarding access to the medications, Justice Stevens limited the scope of the holding in *Whalen*. He made it clear that *Whalen* decided only the case at hand and

---

[395] *Id*. at 603. "The record supports the conclusion that some use of [the] drugs has been discouraged . . . [but] about 100,000 prescriptions for such drugs were being filled each month prior to the entry of the District Court's injunction [but after the enactment of the statute]."

[396] *Id.*

[397] *Id.*

did not "decide any question which might be presented by the unwarranted disclosure of accumulated private data whether intentional or unintentional or by a system that did not contain comparable security provisions."[398]

Thus *Whalen* did no more than assert that there is a right to avoid the disclosure of one's personal information by the government. The exact source of the right and its parameters were left undefined. It thus falls to other courts to determine what constitutes a "serious invasion" of one's information privacy rights, and the appellate decisions discussed below have begun to shape the parameters of the privacy-as-confidentiality conceptualization of privacy.

In the same year *Whalen* was decided, Justice William Brennan wrote the majority opinion in the second landmark case that even more firmly established the individual privacy interest in avoiding the disclosure of personal matters by the government or the right to confidentiality, *Nixon v. Administrator of General Services*.[399] Like *Whalen*, *Nixon* involved a constitutional challenge to a statute on privacy grounds. Former President Richard M. Nixon had challenged the Presidential Recordings and Materials Preservation Act[400] on a number of grounds[401] including that certain provisions of the Act invaded his privacy.

---

[398] *Id.* at 605-06.

[399] 433 U.S. 425 (1977).

[400] 44 U.S.C. § 2107 (1970 ed., Supp. V).

[401] He alleged that the "archival screening" process outlined in the Act was a violation of presidential privilege, a violation of the separation of powers, and a violation of his First Amendment associational rights, and he alleged the process was an unconstitutional bill of attainder. The Court found against the former President on all of these grounds as well as on the question of whether the process was an unconstitutional invasion of his privacy.

The Act provided rules used to guide the process of preparing the immense number of documents and recordings generated by a presidential administration for storage in a presidential library. Part of this process involved "archival screening," which was the process of separating the President's personal information from the millions of pages of public records. When President Nixon argued that this process – granting strangers access to his private papers that were intermixed with the public documents -- constituted an unconstitutional invasion of his privacy, the Court followed *Whalen* and found adequate safeguards among the guidelines for archival screening contained within the Act. Stated another way, the Act had provisions to make sure Nixon's personal information remained confidential.

Justice Brennan cited *Whalen* and acknowledged, "One element of privacy has been characterized as 'the individual interest in avoiding disclosure of personal matters'"[402] and noted that "public officials, including the President, are not wholly without constitutionally protected privacy rights in matters of personal life unrelated to any acts done by them in their public capacity."[403] Quoting *Katz v. United States*, Justice Brennan granted that the President had a "legitimate expectation of privacy."[404]

As was the case in *Whalen*, the statute was subjected to substantive due process review and part of this process involved balancing the invasion of former President Nixon's privacy against "the public interest in subjecting the Presidential materials of

---

[402] Nixon v. Adm'r of Gen. Serv's. 433 U.S. 425, 457 (1977). Here Brennan cited the district court's finding that "Presidents who have established Presidential libraries have usually withheld matters concerned with family or personal finances, or have deposited such materials with restrictions on their screening."

[403] *Id.*

[404] *Id.*

appellant's administration to archival screening."[405] Justice Brennan framed the elements to be weighed when he wrote:

> [T]he constitutionality of the Act must be viewed in the context of the limited intrusion of the screening process, of appellant's status as a public figure, of his lack of any expectation of privacy in the overwhelming majority of the materials, of the important public interest in preservation of the materials, and of the virtual impossibility of segregating the small quantity of private materials without comprehensive screening.[406]

Justice Brennan compared safeguards in the Presidential Recordings and Materials Preservation Act to the types of safeguards the Court validated in the New York statute under review in *Whalen*. He wrote, "Not only does the Act challenged here mandate regulations similarly aimed at preventing undue dissemination of private materials but, unlike *Whalen*, the Government will not even retain long-term control over such private information; rather, purely private papers and recordings will be returned to appellant under [provisions] of the Act."[407] In *Whalen*, personal information would be retained for five years in paper form and indefinitely in the computerized databases.

In *Nixon* the Court held that the infringement upon President Nixon's privacy was constitutional because of the public interest in removing his personal information from the vast sum of public records and because the Act "provides procedures and orders the promulgation of regulations expressly for the purpose of minimizing the intrusion into

---

[405] *Nixon*, 433 U.S. at 458.

[406] *Id.* at 465. Justice Brennan said: "[The] appellant cannot assert any privacy claim as to the documents and tape recordings that he has already disclosed to the public . . . . Most of the 42 million pages were prepared and seen by others and were widely circulated within the Government." President Nixon conceded "that he saw no more than 200,000 [personal] items." Ultimately, Justice Brennan said: "The vast majority of the materials in question were previously shared, public records. . . . [T]he appellant's privacy claim embracing . . . 'extremely private communications between him and . . . his wife, his daughters, his physician, lawyer, and clergyman, and his close friends, as well as personal diary dictablets and his wife's personal files,' relates only to a very small fraction of the massive volume of official materials with which they are presently commingled." *Id.* at 459.

[407] *Id*. at 458-59.

appellant's private and personal materials."[408] Another factor that weakened President Nixon's privacy claim was the fact that "any intrusion by archivists into appellant's private papers and effects is undertaken with the sole purpose of separating private materials to be returned to appellant."[409] In *Whalen* the materials would be stored longer and used as evidence against private individuals in criminal court.

Thus, in both *Whalen* and *Nixon*, the Supreme Court established that individuals are entitled to a constitutionally protected privacy interest in avoiding the disclosure of personal matters by the government or, stated differently, an interest in confidentiality. Though the parameters of this right remained undefined, in both decisions the Court relied upon substantive due process review in the form of a balancing test that weighed the government's interest in accessing the information against one's privacy interest in the information. The Court hasex plicitly recognized a privacy-as-confidentiality conceptualization by creating a "concomitant duty" on the part of government to safeguard the personal information it compels citizens to disclose One aspect of an individual's information privacy interest is to expect these safeguards when surrendering personal information.

One other Supreme Court case has become a key part of information privacy doctrine, the decision in *Paul v. Davis*.[410] In *Paul*, the name and photograph of an individual who had been arrested but not yet convicted of shoplifting had been placed on a flyer that identified him as a shoplifter. The flyers were then distributed to more than

[408] *Id.* at 459.

[409] *Id.* at 462.

[410] 424 U.S. 693 (1976).

800 retailers.[411] The plaintiff claimed, among other things, that the flyer was a "violation of a right to privacy guaranteed by the First, Fourth, Fifth, Ninth, and Fourteenth Amendments."[412] Justice William H. Rehnquist wrote the opinion in *Paul* and held:

> While we have in a number of our prior cases pointed out the frequently drastic effect of the "stigma" which may result from defamation by the government in a variety of contexts, this line of cases does not establish the proposition that reputation alone, apart from some more tangible interests such as employment, is either "liberty" or "property" by itself sufficient to invoke the procedural protection of the Due Process Clause.[413]

This language is often cited by the U.S. Circuit Courts of Appeal in information privacy cases when the courts must decide which types of information are entitled to protection under *Whalen*. *Paul* effectively eliminates embarrassing but not highly personal information. Moreover, *Paul* also provided guidance as to what types of information should be protected. Justice Rehnquist reasoned:

> In *Roe* the Court pointed out that the personal rights found in this guarantee of personal privacy must be limited to those which are fundamental or "implicit in the concept of ordered liberty." . . . The activities detailed as being within this definition were . . . matters relating to marriage, procreation, contraception, family relationships, and child rearing and education.[414]

Lower courts cite *Paul* in concluding that personal information that closely relates to these fundamental areas is more likely to be protected under a constitutional right of

---

[411] *Id.* at 694-96. In late 1972 two police departments had agreed to combine their efforts for the purpose of alerting local area merchants to possible shoplifters who might be operating during the Christmas season. The flyers were part of the effort. At the time petitioners caused the flyer to be prepared and circulated respondent had been charged with shoplifting but his guilt or innocence of that offense had never been resolved. Shortly after circulation of the flyer, the charge against respondent was finally dismissed by a judge of the Louisville Police Court.

[412] *Id.* at 712.

[413] *Id*. at 701.

[414] *Id.* at 713.

confidentiality than is information related to more common areas such as finances. The further removed from intimate circumstances such as childbirth or marriage, the less likely it is that the information will be entitled to constitutional protects.

Therefore, as of 1978, the U.S. Circuit Courts of Appeal had only three guideposts for deciding information privacy cases. First, individuals had a right to avoid the disclosure of personal matters by state actors. Second, that right involved a duty on the part of government to protect the information that it had compelled individuals to surrender. Lastly, the appropriate form of judicial review should involve a balancing test weighing the government's interest in collecting personal information against the resulting infringement upon individual privacy rights. The following discussion will illuminate how the lower courts have started to conceptualize privacy as a right to confidentiality in information privacy cases For purposes of analysis, the circuit court cases have been grouped into two general categories: the first contains cases that involve challenges to statutes, subpoenas, and disclosure agreements, and the second contains cases involving challenges to the actions of public officials. Each category of cases has its own form of legal analysisas is discussed below .

Challenges to Statutes, Subpoenas, and Disclosure Agreements

In information privacy cases that involve a challenge to an ordinance, statute, or policy that has allegedly infringed upon an individualinformation privacy right, the circuit courts apply substantive due process.[415] The constitutionality of a particular law is

[415] BLACK'S LAW DICTIONARY 539 (8th ed. 2004). "The doctrine that the Due Process Clauses of the 5th and 14th Amendments require legislation to be fair and reasonable in content and to further a legitimate governmental objective."

determined by balancing any infringements caused by the law against those interests the government has advanced to justify the legislation.[416] This balancing approach has been used in privacy jurisprudence since *Griswold v. Connecticut*[417] and has consistently been used to determine the constitutionality of statutes that in some way prevent individuals from making certain personal decisions.[418] Since *Whalen* distinguished the privacy interest in avoiding the disclosure of personal information from decisional privacy, the circuit courts have also adopted substantive due process to review statutes that compel individuals to surrender personal information to the government.

This section discusses eleven U.S. Circuit Courts of Appeal cases that have defined the scope of what the Fifth Circuit termed one's privacy interest in confidentiality[419] as well as the level of judicial review that should be applied in such cases. Three cases involved challenges to statutes that compelled disclosure of personal information from individuals.[420] Three were challenges to subpoena power granted under

---

[416] *See* Myer v. Nebraska, 262 U.S. 390, 399-400 (1923). "The established doctrine is that [liberty as guaranteed by the Fourteenth Amendment] may not be interfered with, under the guise of protecting the public interest, by legislative action which is arbitrary or without reasonable relation to some purpose within the competency of the state to effect. Determination by the Legislature of what constitutes proper exercise of police power is not final or conclusive but is subject to supervision by the courts."

[417] 318 U.S. 479 (1965).

[418] *See* Washington v. Glucksburg, 521 U.S. 707 (1997)(upholding Washington's law that makes it a crime to assist in a suicide), Cruzan v. Director, Missouri Department of Health, 457 U.S. 261 (1990) (the Court held that there is no constitutional bar to a State establishing a procedural requirement that requires evidence of the patient's, as opposed to surrogate family members', intention to forgo treatment), Moore v. City of East Cleveland, 431 U.S. 494 (1977) (ruling that an ordinance had drawn the definition of 'family" too narrowly and prohibited, among other combinations, uncles from living in the same residences as nephews), *and* Roe v. Wade, 410 U.S. 113 (1973) (striking down a Texas statute making it illegal to procure an abortion unless it is medically prescribed or performed to save the life of the mother).

[419] Plante v. Gonzales, 575 F.2d. 1119 (5th Cir. 1978) (labeling the privacy interests in *Whalen* as confidentiality (disclosure of personal matters) and autonomy (making certain kinds of important decisions)). These terms have been adopted and are widely used in circuit court information privacy decisions.

[420] *Id.* (dealing with a claim by five Florida state senators that the financial disclosure provisions within Florida's Sunshine Amendments, Article II, § 8(h)(1) violated their privacy rights), Barry v. City of New

both state and federal statutory authority.[421] Two concerned situations in which the federal government attempted to compel the disclosure of information from federal employees,[422] and one that concerned personal information that was generated during pretrial discovery.[423] Lastly, two cases from the Sixth Circuit are discussed.[424] The Sixth Circuit is the only circuit to reject a balancing test as the appropriate form of substantive due process review in information privacy law.

The Standard of Review

Despite general recognition that, in the words of Fifth Circuit Judge John Minor Wisdom, "[i]n *Whalen* the Court made an effort to unsnarl some of the tangled strands of privacy,"[425] opinions from the circuit courts reflect some frustration with the Supreme

---

York, 712 F.2d. 1554 (2nd Cir. 1983) (deciding a challenge by New York City Firefighters and Police Officers to a New York City ordinance, LOCAL LAW 48, NEW YORK CITY ADMIN. CODE, amending LOCAL LAW 48, NEW YORK CITY ADMIN. CODE § 1106-5.0, that required certain city employees to submit annual financial reports to the City Clerk's office, which would then be made available to the public), *and* Russell v. Gregoire, 124 F.3d 1079 (9th Cir. 1997) (involving a challenge to the registration and disclosure provisions of the Washington State sex offender registry law, WASH. LAWS, Ch. 3, §§ 401, 116).

[421] Schacter v. Whalen, 581 F.2d 35 (2d Cir. 1978) (involving a challenge to the subpoena power of the New York State Board for Professional Conduct); United States v. Westinghouse Electric Corporation, 638 F.2d 570 (3rd Cir. 1980) (involving a challenge to the subpoena power of the National Institute of Occupational Safety and Health (NIOH)); and Fadjo v. Coon, 633 F.2d 1172 (5th Cir. 1981) (challenging the confidentiality of information obtained by subpoena under Florida State law, FLA. STAT. ANN. § 119.07(2)(C) & (I)).

[422] Nat. Fed'n. of Fed. Employers v. Greenberg, 983 F.2d 286 (D.C. Cir. 1993) (concerning three questions on a questionnaire, DD Form 398-2, that all federal employees with security clearances at or above the "secret" level were asked to answer); Denius v. Dunlap, 209 F.3d 944, 955 (7th Cir. 2000) (concerning a mandatory financial disclosure form to be signed by employees of a government program that provided education for high school drop-outs).

[423] Tavoulareas v. Washington Post Co., 724 F.2d 1010 (D.C. Cir. 1984) (concerning sensitive commercial information surrendered by Mobil Oil Co. as part of the discovery process in a defamation suit).

[424] J.P. v. DeSanti, 653 F.2d 1080 (6th Cir. 1981); Cutshall v. Sundquist, 193 F.3d 466 (6th Cir. 1999).

[425] Plante v. Gonzales, 575 F.2d 1119, 1128 (5th Cir. 1978).

Court's decisions in *Whalen* and *Nixon*. The Supreme Court had recognized that a right to avoid the disclosure of personal information was rooted in the Constitution,[426] but, as Judge Wilfred Feinberg of the Second Circuit lamented, the "nature and extent of the interest . . . and the appropriate standard of review for alleged infringements of that interest remain unclear."[427] Judge A. Raymond Randolf, writing for the D.C. circuit in *National Federation of Federal Employers v. Greenberg*,[428] wrote, "When we return to *Whalen* and look behind the Supreme Court's general remark . . . we find ambiguity."[429] In completely rejecting the constitutional right to confidentiality, Sixth Circuit Judge Cornelia G. Kennedy asserted that there is yet no "clear indication from the Supreme Court" regarding the privacy interest in avoiding disclosure and that dicta in *Whalen* and *Nixon* were "isolated statements" from which she could not "recognize a general constitutional right to have disclosure of private information measured against the need for disclosure."[430]

---

[426] *See Westinghouse*, 638 F.2d at 577 (holding that "the privacy interest asserted in this case falls within the first category referred to in *Whalen v. Roe*, the right not to have an individual's private affairs made public by the government); *Tavoulareas*, 724 F.2d at 1019 (referring to *Whalen* in holding that "recent Supreme Court decisions indicate that a litigant's interest in avoiding public disclosure of private information is grounded in the Constitution itself, in addition to federal statutes and the common law); and Denius v. Dunlap, 209 F.3d 944, 955 (7th Cir. 2000) (referring to *Whalen* in recognizing that "the 'concept of ordered liberty' protected by the Fourteenth Amendment's Due Process Clause has been interpreted to include 'the individual interest in avoiding disclosure of personal matters'").

[427] Barry v. City of New York, 712 F.2d. 1554, 1559 (2nd Cir. 1983); *see also* Westinghouse, 638 F.2d at 577 (criticizing the right to avoid disclosure, as recognized in *Whalen* and *Nixon*, because the "full measure of the constitutional protection of the right to privacy is unclear").

[428] 983 F.2d 286 (D.C. Cir. 1993).

[429] Judge Randolf asked rhetorically; "What 'individual interests' receive protection from disclosure? Plaintiffs suggest the interest in avoiding humiliation or embarrassment entailed in the disclosure of personal information. What 'personal information' and disclosure to whom? To the government as employer or to the world? However one defines the scope of the protection, what are the provisions in the Constitution that are said to confer it?" *Id.* at 293.

[430] J.P. v. DeSanti, 653 F.2d 1080, 1089 (6th Cir. 1981).

The fact that *Whalen* apparently established a right but failed to indicate what information was protected, in what circumstances, and to what degree was not only a frustration to judges, but plaintiffs too seemed to struggle with their attempts to mount constitutional challenges based upon this right. For instance, in the Ninth Circuit case of *Russell v. Gregoire*,[431] Judge Diarmuid F. O'Scannlain complained that the plaintiffs' case relied solely upon an interpretation of *Whalen* and *Nixon* by which they hold that the "mere collection of private information may constitute a violation of a constitutional right to privacy."[432] He upheld the statute in question partly because the plaintiffs could not "pinpoint the source of the [privacy interest at stake] or identify its contours . . . and they fail to explain precisely how the Act violates it beyond collating and releasing information."[433] Judge Randolf lamented that the plaintiffs' brief in *Greenberg* referred "to nothing more specific than '[t]he Constitution' as the foundation for this constitutional right."[434]

The circuit courts must not only identify the source and scope of the confidentiality branch of constitutional privacy protections, but they also must develop the appropriate form of substantive due process review for information privacy cases. For

---

[431] 124 F.3d 1079 (9th Cir. 1997). This case was a challenge to the registration and disclosure provisions of the Washington State Community Protection Act , 1990 WASH. LAWS, ch. 3.§§ 401, 116 (1990), which applies only to those with sex offender status.

[432] 124 F.3d. at 1093

[433] *Id.* Judge O'Scannlain asserted that they misinterpreted the Supreme Court because "neither [case] established a general constitutional right to privacy in information collected in a database."

[434] Nat. Fed'n. of Fed. Employers v. Greenberg, 983 F.2d 286, 293 (D.C. Cir. 1993). Judge Randolf actually expressed gratitude that since the case involved a facial challenge, "[T]his case does not require any extended survey of this uncharted terrain." A facial challenge means that if any legitimate purpose for the statute can be identified, it will be allowed to stand. No substantive review of information privacy law was required in the case.

instance, in *Plante v. Gonzales*,[435] a case cited often by the other circuits, Judge Wisdom saw the primary problem to be solved by the Fifth Circuit as "to determine the proper standard of review of their claims, then apply it."[436] He noted, "The Court has avoided proclaiming such a standard in the two cases raising the issue in which it issued opinions, *Whalen v. Roe* and *Nixon v. Administrator of General Services*"[437] He decided that in the Fifth Circuit "the constitutionality of the [statute] will be determined by comparing the interests it serves with those it hinders."[438]

In adopting this balancing standard as an intermediate level of judicial scrutiny, Judge Wisdom reasoned:

> [A] balancing standard seems appropriate. . . . [A]n application of strict scrutiny would draw into question many common forms of regulation, involving disclosure to the public and disclosure to government bodies. . . . [Yet], scrutiny is necessary. . . . Something more than mere rationality must be demonstrated. Otherwise, public disclosure requirements such as Florida's could be extended to anyone, in any situation.[439]

In *Barry v. City of New York*,[440] Judge Wilfred Feinberg first noted "Most courts considering the question appear to agree . . . that some form of intermediate scrutiny or

---

[435] 575 F.2d 1119 (5th Cir. 1978).

[436] Plante v. Gonzales, 575 F.2d 1119, 1132 (5th Cir. 1978). Judge Wisdom first eliminated the senator's privacy interest from the *Whalen* privacy interest in "independence in making certain kinds of decisions." He noted: "Disclosure laws, unlike laws banning contraception, miscegenation, or abortion, do not remove any alternatives from the decision-making process." He thus wrote "[F]inancial disclosure may . . . have some influence on intimate decision-making, [but] we conclude that any influence does not rise to the level of a constitutional problem." I*d*. at 1131.

[437] *Id.* at 1134

[438] *Id.*

[439] *Id.*

[440] 712 F.2d. 1554 (2d Cir. 1983).

balancing approach is appropriate as a standard of review." He then decided the appropriate level of judicial review was intermediate scrutiny, a balancing test in which the government's interest in collecting the financial information [from plaintiffs] is weighed against the individual privacy interest involved.[441] In a later Fifth Circuit decision, *Fadjo v. Coon*,[442] Judge Robert Smith Vance cited Judge Wisdom's decision in *Plante* to firmly establish the use of a balancing test in the Fifth Circuit. He wrote, "An intrusion into the interest in avoiding disclosure of personal information will . . . only be upheld when the government demonstrates a legitimate state interest which is found to outweigh the threat to the plaintiff's privacy interest."[443]

Judge Edward A. Tamm wrote the D.C. Circuit opinion in *Tavoulareas v. Washington Post*.[444] Unlike Judges Wisdom and Vance, he thought *Nixon* clearly established intermediate scrutiny as the appropriate level of review in information privacy cases. He noted that the opinion in *Nixon* was written by Justice Brennan who held "that the constitutional right to nondisclosure is rooted primarily in the fourth amendment."[445] Since Fourth Amendment adjudication typically involves a balancing of the state's interests in infringing upon individual privacy (probable cause) against the

---

[441] *Id.* at 1559.

[442] 633 F.2d 1172 (5th Cir. 1981).

[443] Fadjo v. Coon, 633 F.2d 1172, 1176 (5th Cir. 1981).

[444] 724 F.2d 1010 (D.C. Cir. 1984).

[445] *Id.* at 1020; *see also id*. at 1019 (citing *Whalen*: "Broad dissemination by state officials of such information . . . would clearly implicate constitutionally protected privacy rights, and would presumably be justified only by compelling state interests" which established that strict scrutiny might be applied in certain circumstances).

value of that privacy right, he reasoned that this was the form of scrutiny the courts should adopt for substantive due process privacy analysis.

Thus, judicialreview would require the circuit courts, in information privacy cases, to first define both the individual privacy interest and the government interest in disclosure and then weigh them against one another. In the cases that follow, an information privacy calculus begins to emerge. Were it to be written as a two step algebraic expression, it would appear like this:

(*Type of Information* + *Plaintiff Category*) – *Government Safeguards* = *Individual Privacy Interest*

Individual Privacy Interest (>,<) *Government Interest in Information* = Decision

The Individual Privacy Interest

In applying this balancing test, the circuit courts must first establish the individual privacy interest that is at risk. A process for doing this is emerging from the various circuit court decisions. First the court evaluates the type of information at risk and determines the level of constitutional protection to which such information is entitled. Next, the plaintiff category is evaluated. The court determines whether circumstances exist that limit the level of privacy protection to which a plaintiff is entitled, such as he or she being a candidate for office or convicted felon. Lastly, the court considers the extent to which information safeguards being used by the government lessen the risk to this privacy interest. This section will draw upon U.S. Circuit Courts of Appeal cases to illustrate how these three elements have been combined to define individual privacy interests.

Types of Information

Typically, the courts will first consider the type of information being disclosed. Based on the Supreme Court's decision in *Paul*, lower courts have ruled that the more closely information relates to the fundamental interests traditionally protected by decisional privacy rights (marriage, procreation, intimate relationships, etc.), the more constitutional protection the information deserves. Among the circuit courts, the decisional privacy rights are referred to as the "autonomy" branch of privacy.

Among the statutory challenges discussed here, the court has weighed types of information including financial information, medical information, and sensitive commercial data. A ranked continuum of protected information is emerging from the circuit court cases. Medical information that is related to procreation, familial relationships, and sexual preference as well as commercial information that is vital to the continued existence of a corporation have been afforded the highest level of protection. More general medical information and financial information are entitled to a middle level of protection. Lastly, information that is a matter of public record, such as one's sex offender status, receives the least amount of protection. A few examples are discussed here.

In *United States v. Westinghouse Electric Corporation*,[446] Circuit Judge Dolores Korman Sloviter upheld a subpoena for employee medical records that had been issued to Westinghouse by the National Institute of Occupational Safety and Health (NIOSH). Westinghouse refused to surrender records for employees working in a particular section

[446] 638 F.2d 570 (3rd Cir. 1980).

of a Pennsylvania plant to NIOSH, so the institute issued the subpoena.[447] In determining the appropriate level of protection for these records, the court considered a number of factors, including that individuals commonly share personal information with a wide variety of medical personnel (doctors, pharmacists, insurance companies, counselors, etc.), so, invoking the third-party doctrine, Judge Sloviter held that the information was not entitled to as high a level of protection as is reserved for information that is kept secret and never shared. Nevertheless, she distinguished the information at issue in *Westinghouse* from that in *Whalen*. Judge Sloviter recognized that the medical information subpoenaed in *Westinghouse* was "more extensive than the mere fact of prescription drug usage by identified patients considered in [*Whalen*] and may be more revealing of intimate details. Therefore, we hold that it falls within one of the zones of privacy entitled to protection."[448]

Because the information in *Westinghouse* was extensive and despite the third-party doctrine, Judge Sloviter strongly suggested that NIOSH "give prior notice to the employees whose medical records it seeks to examine and to permit the employees to raise a personal claim of privacy, if they desire."[449] Thus, though she had found the

---

[447] *Id.* at 572. NIOSH initiated the request following a request from the International Union of Electrical Workers, Local 601, which alleged that "workers were suffering allergic reactions as a result of exposure to methyl ethyl ketone. After repeated requests for medical records of both present and past employees who worked with the substance, NIOSH issued a subpoena duces tecum (a subpoena that requests the surrender of named documents). Westinghouse first refused to honor the subpoena and then later offered conditional compliance. It was this refusal to fully comply with the subpoena that led to this case.

[448] *Id.* at 577. She wrote that "there can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection."

[449] *Id.* at 581.The Third Circuit suggested that "[the notice] should contain information as to the fact and purpose of the investigation and the documents NIOSH seeks to examine, and should advise the employees that if they do not object in writing by a date certain, specifying the type of material they seek to protect, their consent to disclosure will be assumed."

subpoena constitutional, Judge Sloviter sought to reinforce the ability of employees to control access to their personal information by providing procedural protections to each employee who judges "the information so sensitive that it outweighs that employee's interest in assisting NIOSH in a health hazard investigation."[450]

Judge Edward A. Tamm made a similar decision regarding sensitive commercial information in *Tavoulareas v. Washington Post Company*.[451] The case dealt with an attempt by the *Washington Post* to unseal sensitive commercial documents and testimony that had been surrendered by Mobil Oil Company during the discovery phase of a defamation suit.[452] Prior to the trial, Mobil was granted a protective order to secure the confidentiality of the commercial information sought by the *Post*.

Mobil had argued that it needed to protect the materials "to avoid impairing the competitive position of Mobil, . . . to afford it reasonable protection against disclosure of proprietary and confidential business information [and] also to minimize the possibility of impairing Mobil's relationship with the Government of the Kingdom of Saudi Arabia."[453] The court reasoned that if Mobil's relationship with Saudi Arabia were damaged, the corporation's ability to successfully compete in the marketplace would be compromised. Consequently, after holding that a corporation had a constitutionally protected privacy interest in avoiding the disclosure of sensitive commercial information, Judge Tamm wrote, "We have determined . . . that Mobil's justification . . . was sufficient

---

[450] *Id.*

[451] 724 F.2d 1010 (D.C. Cir. 1984).

[452] The president of Mobil Oil Company and his son filed a libel suit against the *Washington Post* for defamatory content in two articles that alleged that the younger Tavoulareas achieved his position and subsequent success through nepotism.

[453] *Tavoulareas*, 724 F.2d at 1012.

to show the disputed documents contained information of the kind deserving constitutional protection."[454]

Whereas the commercial information in *Tavoulareas* was considered vital to the very existence of the corporation, the circuit courts have not assigned the same level of importance to individuals' personal financial information. In *Plante*, Judge John Minor Wisdom considered the plaintiffs' privacy interest in their financial information to be "substantial" and acknowledged that "privacy of personal matters is an interest in and of itself, protected constitutionally."[455] Nevertheless, central to his holding was the notion that those interests protected under the autonomy branch of privacy were entitled to a higher level of constitutional protection than were interests under the "confidentiality" branch of privacy, protections that allow individuals to avoid the disclosure of personal matters.

Judge Wisdom noted that the plaintiffs in *Plante* argued that financial information was tied to the fundamental familial interests the Supreme Court prioritize in *Paul* -- "matters relating to marriage, procreation, contraception, family relationships, and child rearing and education."[456] Judge Wisdom opined, "The senators are well advised to try to tie their charges to domestic matters."[457] However, he distinguished the Florida Sunshine

---

[454] *Id.* at 1025.

[455] Plante v. Gonzales, 575 F.2d 1119, 1135 (5th Cir. 1978).

[456] Paul v. Davis, 424 U.S. 693, 713 (1976).

[457] *Plante*, 575 F.2d at 1128. Here Judge Wisdom is reviewing the plaintiff's legal argument that the financial disclosure provisions are directly tied to the decisional/familial privacy interests protected under *Paul*. His summary of the plaintiffs' position is thus: "The nature of financial investments, their wisdom, worth or desirability are matters decided by family councils for the family's benefit. Whether they should be exposed or protected from exposure is a matter of great family concern. Media publication of disclosed wealth can bring mischief, even kidnappers or other criminal attention to an office holder. Financial privacy

Amendments from those interests in traditional decisional privacy cases such as *Roe v. Wade*. He reasoned:

> Disclosure laws, unlike laws banning contraception, miscegenation, or abortion, do not remove any alternatives from the decision-making process. Their effect on financial decisions is more indirect. They might deter some decisions. More basically, however, disclosure laws do not involve decisions as important as those in the earlier decided cases.[458]

Judge Wisdom also limited the scope of privacy protections for financial information by invoking the third-party doctrine, just as the Third Circuit did with medical information in *Westinghouse*. He wrote: "Our society has long regulated people's finances. Interference with business activity, through licensing, taxing, and direct regulation, is common. All these governmental actions impinge on the ability of the individual to order his financial affairs. They do so directly. The indirect effects caused by financial disclosure pale by comparison."[459]

Moreover, in 1983 the Second Circuit used similar reasoning. In *Barry v. City of New York*,[460] a group composed of New York City firefighters and police officers claimed that a local ordinance that required city employees to submit annual financial reports to the City Clerk's office, which then made the submitted reports available to the

---

is and ought to be protected from governmental intrusion . . . in the manner that marital and family privacy is protected."

[458] *Id.* at 1130-31. Judge Wisdom said: "Nor can [disclosure laws] be protected as incident to protection of the family. The appropriate question is: What impact will financial disclosure have upon the way intimate family and personal decisions are made? Will it affect the decision whether to marry? Will it determine when or if children are born? There is no doubt that financial disclosure may affect a family, but the same can be said of any government action. While disclosure may have some influence on intimate decision-making, we conclude that any influence does not rise to the level of a constitutional problem."

[459] *Id.*

[460] 712 F.2d. 1554 (2d Cir. 1983).

public violated their right to keep their financial records confidential. Judge Fienberg held that the financial disclosures, though they might force one spouse to reveal private financial habits to the other, did not implicate the protections of the "autonomy" branch of the constitutional privacy interests. Judge Feinberg cited *Plante* and held: "It is unclear whether financial disclosure laws significantly implicate any interests protected by the autonomy strand of the right to privacy. The Fifth Circuit has concluded that the autonomy interest does not cover 'financial privacy.'"[461] *Plante* and *Barry* thus held that financial information was not entitled to the highest levels of constitutional protection because it is not related closely enough to fundamental familial interests.

The individual privacy interest in information already in the public record, such as arrest records, is the weakest. In 1997, the Ninth Circuit reviewed a challenge to a Washington State law that required sex offenders to register personal information and allowed the state to disclose that information to the public. Judge Diarmuid O'Scannlain held that the type of information collected and revealed under the Act could not be protected. He wrote, "The information collected and disseminated by the Washington statute is already fully available to the public and is not constitutionally protected."[462]

Conversely, in *Tavoulareas*, Judge Tamm noted that in the discovery process, individuals are forced by the court to disclose the kind of personal information deserving privacy protection under these decisions. Thus, he reasoned that an individual's constitutional privacy interest can be implicated by the discovery process to the same extent it is implicated by disclosure requirements of statutes. In both instances, the

[461] *Id.* at 1559.

[462] Russell v. Gregoire, 124 F.3d 1079, 1094 (9th Cir. 1997).

government is forcing disclosure of personal information.[463] In *Tavoulareas*, sensitive commercial information compelled during discovery and not used in trial was allowed to remain confidential under a protective order.

Plaintiff Categories

Once the type of information at issue has been categorized, the courts' analyses typically move to the second factor, the plaintiff category. The emerging plaintiff categories somewhat mirror plaintiff categories from other legal areas, such as defamation law. By default, private persons seem to be entitled the highest level of constitutional protection, government employees to a moderate level, elected public officials to little protection, and criminals to the least amount.

In *Plante,* Judge Wisdom noted that the Sunshine Amendments under review applied specifically to public officials who had voluntarily placed themselves in the public eye. He recognized a distinct plaintiff category in information privacy law when he wrote: "Plaintiffs in this case are not ordinary citizens, but state senators, people who have chosen to run for office. . . . It does put some limits on the privacy they may reasonably expect."[464] He summarized his overall evaluation of the privacy interest being weighed when he wrote: "Financial privacy is a matter of serious concern, deserving strong protection. . . . [P]ublic interests supporting public disclosure for these elected

[463] Tavoulareas v. Washington Post Co., 724 F.2d 1010, 1020-21 (D.C. Cir. 1984).

[464] *Plante*, 575 F.2d at 1135.

officials are even stronger. . . . [M]andatory financial disclosure for elected officials is constitutional."[465]

In *Tavoulareas*, Judge Tamm also broke new ground regarding information privacy plaintiff categories when he held that a corporation could claim a constitutional right to avoid the disclosure of sensitive commercial information. Following a review of relevant case law he concluded, "[W]hile corporations do enjoy privacy protection under the fourth amendment that protection is qualified to allow adequate policing of corporate conduct."[466] Therefore, when a corporation is compelled to surrender sensitive information to the government for reasons other than policing corporate conduct, it has a constitutional right to confidentiality in that information.

In the other cases, the formation of plaintiff categories was very closely tied to the government's stated interest in collecting information. For instance, in *Barry*, the Second Circuit evaluated the constitutionality of a local ordinance[467] enacted by the New York City Council that required city employees making over $30,000 annually to submit annual financial reports to the City Clerk's office. The reports were to be made available for public inspection. The financial reporting requirements were upheld because these

---

[465] *Id.* at 1136.

[466] *Tavoulareas*, 724 F.2d at 1022 (citing *United States v. Morton Salt Co.,* 338 U.S. 632, 652 (1950) as holding that "the government must be free to ensure that corporate behavior is consistent with the law and the public interest" and "corporations must disclose information to regulatory agencies so long as the demand is not too indefinite and the information sought is reasonably relevant"). Discovery, however, is not conducted to police or regulate litigants, but to prepare for the trial of a dispute. The purpose of discovery is not affected by the fact that a party to the suit is a corporation. Therefore, in the context of confidential discovery materials not used at trial, a corporation's privacy interest in nondisclosure is essentially identical to that of an individual. *id.*

[467] LOCAL LAW 48, NEW YORK CITY ADMIN. CODE AMENDING LOCAL LAW 1, NEW YORK CITY ADMIN. CODE § 1106-5.0.

individuals were paid with tax dollars and citizens had an interest in knowing how there tax dollars were allocated and in eliminating any corruption that the disclosure revealed.

Similarly, *Greenberg*[468] involved a facial challenge to three questions on the "National Agency Questionnaire,"[469] which all federal employees holding security clearances at or above the "secret" level were asked to answer.[470] Because these individuals were entrusted with national secrets and many had a direct role in national security, the court reasoned that the public had a valid interest in learning about their financial, medical, psychological, and criminal backgrounds.

Though these plaintiff categories are taking shape in the wide variety of circuit court information privacy decisions, they are not stand-alone classifications. They are necessarily defined by context. For instance, the federal employees in *Greenberg* had security clearances unlike the federal employee in *Denius v. Dunlap*.[471] *Denius* involved a constitutional challenge to a disclosure agreement that teachers in a government-run program for high school dropouts were asked to sign as a condition of continued employment. Judge Joel Martin Flaum held that the plaintiff was exempt from disclosing financial and medical information because the government had not advanced a legitimate purpose for requiring the disclosure.

---

[468] 983 F.2d 286 (D.C. Cir. 1993).

[469] DD Form 398-2. The questionnaire seeks the information from each individual's entire life and requests that one sign a release for the government to do a complete background check on any of the items on the form. The challenged questions were numbers 18 (criminal arrest history), 19 (credit history), and 20 (mental health and drug and alcohol use history). The questionnaire resulted from a string of highly publicized spying incidents.

[470] *Greenberg,* 983 F.2d at 287. Employees were informed that "failure to furnish the requested information . . . could result in your not being considered for clearance, access, entry into a uniformed service, or assignment to sensitive duties."

[471] 209 F.3d 944 (7th Cir. 2000).

Another example where context shaped the court's consideration of a plaintiff category is the Ninth Circuit decision in *Russell v. Gregoire*[472] in which the court heard an appeal from two convicted sex offenders who had challenged Washington State's Community Protection Act,[473] which had both registration[474] and disclosure[475] provisions. Not all ex-convicts need to register and disclose personal information, but legislators have determined that this category of offenders is a particularly dangerous threat to citizens, and the courts have thus held that sex offenders are entitled to fewer privacy protections.

The Government's Duty

The last component of the individual privacy interest side of the information substantive due process equation is whether and how the government is fulfilling its duty to safeguard the information it has ordered disclosed. Courts consider any statutory or procedural information safeguards when they evaluate the potential risk to an individual's privacy interest. The better the safeguards, the lower the perceived risk. A statute that contains specific guidelines regarding how the government will protect the personal information is much more likely to be found constitutional. This is why, in the equation above, information safeguards are "subtracted" from the plaintiff's side of the equation. A number of constitutional challenges in the circuit courts have failed because of strong

[472] 124 F.3d 1079 (9th Cir. 1997).

[473] 1990 WASH. LAWS, ch. 3.

[474] 1990 WASH. LAWS, ch.3, § 401.

[475] 1990 WASH. LAWS, ch.3, § 116.

measures the government had in place to honor its duty to prevent unwarranted disclosure under *Whalen*.

For instance, in *Barry*, after reviewing the statutory procedure through which employees could file privacy claims, Judge Feinberg concluded, "[W]e think the statute, as strengthened by the privacy claim procedures, [476] withstands constitutional scrutiny even with respect to the broad public inspection requirement."[477] Similarly, in *Schacter,*[478] the Second Circuit justified the constitutionality of a subpoena for patient records largely on the merits of a "coding process" designed to protect patient information.[479] The Second Circuit accepted the coding system as sufficient to satisfy the state's duty under *Whalen* and held that "the provisions under attack do not violate the patients' constitutional rights."[480]

---

[476] *Id.* at 1561-62. Judge Fienberg summarized the privacy claim procedure outlined in the local law. It generally allows individuals the opportunity to challenge the release of specific bits of information when a member of the public requests to access their file. He noted: "An employee filing a financial report may make a claim of privacy with respect to any item of information sought by the City by explaining in writing the reasons for the request . . . . If a privacy claim has been made and someone requests access to the claimant's report, the matter is referred to the Board of Ethics for evaluation . . . . [T]he Board must consider three factors in evaluating a privacy claim: whether the item is highly personal; whether it relates to the claimant's duties; and whether the item involves a possible conflict of interest . . . . We do not think that the right to privacy protects public employees from the release of financial information that is related to their employment or indicative of a possible conflict of interest. Nor do we think the release of information that is not 'highly personal', rises to the level of a constitutional violation."

[477] *Id.* at 1561. *See also id.* at 1562 (explaining that Judge Feinberg evaluated the effectiveness of the privacy claim procedure and noting, "Only three privacy claims [of twenty-six] were denied, apparently because insufficient information was provided in support of the claims," which he accepted as evidence that the privacy procedure was working in the majority of cases).

[478] Schacter v. Whalen, 581 F.2d 35, 37 (2d Cir. 1978).

[479] *Id.*

[480] *Id.* As far as the doctor's claims, the Second Circuit held that his constitutional right to privacy was also not abridged and further noted that Dr. Schacter had less standing to complain than did the patients in *Whalen* because he himself was the subject of an investigation.

In some cases the court engaged in an accounting of precisely how the government would protect the information at issue. For example, in *Westinghouse* the court reviewed specific safeguards:

> Only aggregate data is included in the forms of the study distributed to employees and others. The excerpted data which is retained by NIOSH is maintained in locked cabinets, inside the Medical Section of the agency, in rooms locked during non-office hours. Material from small studies is not placed on computers; data from large studies is removed from the computer after six months. NIOSH has represented that no outside contractors are used for small studies, such as the one in issue here, and that when such contractors are used, they are bound to nondisclosure by their contract with NIOSH.[481]

Conversely, in some circuits, review of statutory safeguards is more of a rubber-stamp; the presence of safeguard provisions is more important than their substance. For example, in *Russell*, Judge O'Scannlain concluded that Washington's law contained "adequate mechanisms" to limit unnecessary disclosures, but only generally noted that "the collection and dissemination of information is carefully designed and narrowly limited."[482]

Thus, the individual privacy interest side of the balancing equation comprises three parts: the type of information being collected, the type of plaintiff filing a claim, and the safeguards the government has in place to protect the information it has collected. Once the court has established that a constitutionally protected privacy interest in avoiding the disclosure of personal matters exists, it must then determine the value of the other side of the equation, the government's interest in collecting the information.

---

[481] 638 F.2d at 580. The statutory source for NIOSH's information handling provisions is 5 U.S.C. § 552a(m).

[482] Russell v. Gregoire, 124 F.3d 1079, 1094 (9th Cir. 1997).

The Government's Interest

In defending a statute, order, or subpoena, the government must claim at least a legitimate (and in some cases substantial or compelling) state interest in compelling individuals to surrender personal information.[483] The circuit courts have held that improving the electoral process; informing citizens to enable self-government; promoting the public's general health, safety, and welfare; and national security to be substantial and sometimes compelling government interests. For instance, in *Plante*, Judge Wisdom concluded that Florida had a substantial interest in improving the electoral process by instilling confidence in the minds of voters through transparency. Florida's Sunshine Amendments provided voters with more information about candidates and implemented reporting procedures intended to lessen the likelihood of corruption or conflicts of interest.[484] Similarly, in *Barry*, Judge Feinberg found that the statute had a "substantial,

[483] Generally, in constitutional law, government interests are considered legitimate, substantial, or compelling. If the court is applying rational basis review, a merely legitimate interest is sufficient to withstand scrutiny (for instance reducing noise pollution). Under intermediate scrutiny, a substantial interest is warranted (for instance protecting public safety). A compelling interest must be demonstrated under strict judicial scrutiny (for instance national security). Though the information privacy doctrine is new, a general tendency is emerging that the more closely related to fundamental values certain information is, the more compelling the state interest must be in order to justify infringing upon information privacy rights.

[484] Plante v. Gonzales, 575 F.2d 1119, 1134-35 (5th Cir. 1978). He summarized the four primary justifications for the Sunshine Amendments: [1] the public's "right to know" an official's interests, [2] deterrence of corruption and conflicting interests, [3] creation of public confidence in Florida's officials, and [4] assistance in detecting and prosecuting officials who have violated the law."[484] (numerals added) In concluding that there was a substantial government interest, Judge Wisdom noted, "Disclosure . . . makes voters better able to judge their elected officials and candidates for those positions . . . . [T]he reporting requirement will discourage corruption [since] sunshine will make detection more likely, [and] the interest in an honest administration is so strong that even small advances are important . . . . Disclosure may not completely remove this doubt. It should help, however. And more effective methods are not obvious." The only justification about which Judge Wisdom expressed some doubt was the amendments' effectiveness in deterring corruption. He wrote, "While misdeeds may be deterred by the need to file either honest or perjurious financial statements, once they have been committed, the statements may well be useless." Nevertheless, he acknowledged the potential effectiveness of three of the four provisions and concluded that the government's interest was legitimate.

possibly even a compelling, state interest . . . . to deter corruption and conflicts of interest among City officers and employees and to enhance public confidence in the integrity of its government."[485] Judge Feinberg held, "Given the magnitude of the City's interests, we think the constitutional balance . . . tips in favor of permitting public disclosure."[486]

Promoting public safety and welfare has also been upheld as a substantial government interest. The *Schacter* court held that the government interest in obtaining patient records as evidence was a necessary component of a "sound state policy . . . investigation of licensed physicians for medical misconduct" and had "as much rational basis and underlying public-interest justification as the statute identifying patients obtaining certain drugs by prescription in *Whalen*."[487] Protecting the health and safety of workers was considered a substantial government interest in *Westinghouse*. Judge Sloviter concluded that NIOSH's interests were sufficiently substantial when measured against the justifications proffered for the statute reviewed in *Whalen*. She wrote: "[T]he interest in occupational safety and health to the employees . . . future employees and the public at large is substantial. It ranks with other public interests which have been found to justify intrusion into records and information normally considered private."[488] National

---

[485] Barry v. City of New York, 712 F.2d. 1554, 1560 (2d Cir. 1983). *See also id.* at 1563 (describing the legislative intent of financial disclosure as function thusly: "public disclosure of financial reports will spur City agencies and officials to be aggressive in their efforts to police corruption, if only for fear that evidence of misconduct might be found in a financial report and publicized by the press, a public interest group, or a vigilant citizen . . . . [and] public disclosure will enhance public confidence in the integrity of City government if only because the reports will demonstrate that most City officials and employees are honest and not subject to conflicts of interest in the performance of their duties").

[486] *Id*. at 1563.

[487] Schacter v. Whalen, 581 F.2d 35, 37 (2d Cir. 1978).

[488] United States v. Westinghouse Electric Corp., 638 F.2d 570, 579 (3rd Cir. 1980).

security was the interest put forth in *Greenberg*.[489] Judge Randolph reasoned, "Substantial debts, with the attendant financial pressure exerted on employees holding security clearances, or on-going mental health problems are, by anyone's light, important elements of the [judgment] in determining whether a person can be trusted to maintain the nation's secrets."[490]

Conversely, in a number of cases, no government interest was put forth. In 1981, Judge Vance wrote the Fifth Circuit opinion in *Fadjo v. Coon*.[491] The court held that, absent a substantial government interest, individuals have a privacy interest in information compelled by subpoena under Florida law and even to a greater degree if they have been promised confidentiality. Fadjo had been subpoenaed to provide information regarding a man's disappearance at sea.[492] He claimed that the information sought by investigators, under the Florida's subpoena power, had involved the most private aspects of his life.[493] Moreover, prior to testifying, he was assured by investigators that "his testimony was absolutely privileged under Florida law[494] and that

---

[489] The questionnaires were the result of recent spying scandals that compromised national security secrets.

[490] Nat. Fed'n. of Fed. Employers v. Greenberg, 983 F.2d 286, 294 (D.C. Cir. 1993).

[491] Fadjo v. Coon, 633 F.2d 1172 (5th Cir. 1981).

[492] Fadjo had been named the beneficiary of six life insurance policies taken out on Kenneth S. Rawdin, the man whose disappearance was being investigated.

[493] *Fadjo*, 633 F.2d at 1176. Judge Vance distinguished *Fadjo* from the Supreme Court's decision in *Paul v. Davis* because it involves the revelation of intimate information obtained under a pledge of confidentiality rather than the dissemination of official information. *See also* Paul v. Davis, 424 U.S. 693, 713 (1976) (explaining that the Court has considered fundamental rights to be "matters relating to marriage, procreation, contraception, family relationships, and child rearing and education" and noting that "in these areas it has been held that there are limitations on the States' power to substantively regulate conduct").

[494] FLA.STAT.ANN. § 119.07(2)(C) & (I). The Florida legislature amended the Public Records Act to exempt from public disclosure "active criminal investigative information" and "criminal investigative information received by a criminal justice agency prior to January 25, 1979." It is clear that the legislature cannot authorize by statute an unconstitutional invasion of privacy.

the contents of his testimony would be revealed to no one."[495] Investigators then revealed information from Fadjo's testimony to a number of private insurance companies investigating the disappearance, and Judge Vance held that no legitimate state purpose existed sufficient to outweigh the invasion into Fadjo's privacy."[496]

In *Tavoulareas*, Judge Tamm's final holding regarding the sensitive commercial information surrendered during discovery but not used at trial was made because of "the absence of a compelling interest supporting disclosure."[497] Likewise, in *Denius*, Judge Flaum never needed to define the scope or contours of Denius' privacy interest because Dunlop, the director of the government program, never offered any justification for the disclosure agreement. Judge Flaum held: "We conclude that this sweeping disclosure requirement, lacking any safeguards against misuse or further disclosure, and supported by no justification, infringes Denius's right of privacy in confidential information."[498]

Once the level of government interest has been established as legitimate, substantial, or compelling, the court will balance it against the individual privacy interest at risk in the case. The court will determine if the government interest is greater than or less than the individual privacy interest at stake. If the government's interest is greater, the legislation, subpoena, or policy in question will likely be ruled constitutional. If the individual privacy interest is found to be more substantial, the legislation, subpoena, or policy will likely be struck down. The information privacy equation for review of statutory challenges is not being uniformly applied by circuit courts. It is offered here as

[495] *Fadjo*, 633 F.2d at 1174, n.3.

[496] *Id.* at 1175.

[497] Tavoulareas v. Washington Post Co., 724 F.2d 1010, 1029 (D.C. Cir. 1984).

[498] Denius v. Dunlap, 209 F.3d 944, 958 (7th Cir. 2000).

a construct to represent how the various elements of judicial review in information privacy law are emerging form the circuit courts and congealing into a new privacy doctrine.

The Sixth Circuit

The Sixth Circuit is the only circuit to have rejected the use of a balancing test in its information privacy cases. In the 1981 case of *J.P. v. DeSanti*,[499] Judge Cornelia G. Kennedy granted review of whether the post-adjudication uses of the juvenile social histories[500] violated a constitutional right to privacy. She relied primarily on *Paul v. Davis*,[501] which established that information entitled to constitutional protection from disclosure typically relates to marriage, procreation, etc. She concluded that the information in the social histories was not intimate enough to reach that level. She further commented that the otherwise "dispositive affect" of *Paul* was "somewhat clouded" by the subsequent decisions in *Whalen* and *Nixon*, which resulted in additional confusion in "their construction by the courts of appeal."[502]

Judge Kennedy criticized the rapid embrace by the other circuit courts of a balancing test as the appropriate method of review for constitutional privacy suits. She

[499] 653 F.2d 1080 (6th Cir. 1981).

[500] *Id.* at 1082. A social history contains "information from a number of sources, including the complaining parties, the juveniles themselves, their parents, school records, and their past records in the juvenile court. They also include any information on record pertaining to other members of the family and any other information that the probation officer thinks is relevant to the disposition of a case before the juvenile court." Following the adjudication of a particular case, the social histories are "kept on file at the juvenile court, where, upon request, [they are] available to 55 different government, social and religious agencies that belong to a 'social services clearinghouse.'" *Id. See also* OHIO R. JUV. P. 32, the Ohio rule of civil procedure that established the use of the social histories.

[501] Paul v. Davis, 424 U.S. 693 (1976).

[502] *J.P,* 653 F.2d at 1088.

wrote, "Some courts have uncritically picked up that part of *Whalen* pertaining to nondisclosure and have created a rule that the courts must balance a governmental intrusion on this 'right' of privacy against the government's interest in the intrusion."[503] Judge Kennedy asserted that there is no indication in the Supreme Court case law that indicates that a balancing test is the appropriate level of review.

Establishing the method of review for the Sixth Circuit, Judge Kennedy wrote, "We do not view the discussion of confidentiality in *Whalen v. Roe* as overruling *Paul v. Davis* and creating a constitutional right to have all government action weighed against the resulting breach of confidentiality."[504] She then stressed that the *Whalen* Court "explicitly refused to address the existence of such a right."[505] Judge Kennedy concluded, "Absent a clear indication from the Supreme Court we will not construe isolated statements in *Whalen* and *Nixon* more broadly than their context allows [in order] to recognize a general constitutional right to have disclosure of private information measured against the need for disclosure."[506]

Justice Kennedy's reasoning seems to have been based upon the fact that the right of information privacy is too general to be practical. She reasoned,"[The Framers] cannot have intended that the federal courts become involved in an inquiry nearly as broad,

---

[503] *Id.* She noted in particular *Plante*, *Westinghouse*, and *Fadjo*.

[504] *Id.* at 1088-89.

[505] *Id.* (citing language from Whalen v. Roe, 429 U.S. 589, 605-06 (1977), which stated, "We ... need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data whether intentional or unintentional" and from Whalen v. Roe, 429 U.S. 589, 608-09 (1977) (J. Stewart, concurring), which stated, "[T]he Court's opinion did not support the proposition that broad dissemination of the information collected by New York would violate the Constitution." She also reviewed *Nixon* and concluded, "*Nixon* does not overrule *Paul v. Davis* and create a general constitutional right of nondisclosure against which government action must be weighed."

[506] *J.P.*, 653 F.2d at 1089.

balancing almost every act of government, both state and federal, against its intrusion on a concept so vague, undefinable, and all-encompassing as individual privacy."[507] Thus, she limited privacy protections for personal information surrendered to government to those personal rights that can be deemed "fundamental" or "implicit in the concept of ordered liberty" as was established in *Paul v. Davis* and *Roe v. Wade*.[508] In *J.P.*, she held, "The interest asserted by appellant class in nondisclosure of juvenile court records . . . [is] 'far afield' from those privacy rights."[509]

In 1999, Sixth Circuit Judge James Leo Ryan wrote the opinion in *Cutshall v. Sundquist*,[510] and he followed Judge Kennedy's reasoning from *J.P.*. The case involved a challenge to the Tennessee Sex Offender Registration and Monitoring Act[511] by Arthur Cutshall, who was convicted for aggravated sexual battery in 1990. The Act contained a registry provision that allowed a local law enforcement agency to "release relevant information deemed necessary to protect the public concerning a specific [registered] sexual offender."[512] The challenge was made on a number of grounds including that the Act violated Cutshall's constitutional right to privacy.[513]

---

[507] *Id.* at 1090.

[508] *Id.*

[509] *Id.*

[510] 193 F.3d 466 (6th Cir. 1999).

[511] TENN. CODE §§c49-39-101 to 108 (1994).

[512] TENN. CODE. § 40-39-106(c).

[513] *Cutshall*, 193 F.3d at 470. Cutshall claimed the Act also violated his right to privacy under the Tennessee State Constitution, violated the double jeopardy clause, was an ex post facto law, violated the Eighth Amendment as a form of cruel or unusual punishment, and violated the due process and equal protection clauses as well as violated his right to travel interstate. The Sixth Circuit held that since the purpose of the Act was regulatory and not punitive, it did not violate protections against double jeopardy, ex post facto laws, and was not an unconstitutional bill of attainder.

Judge Ryan relied upon *J.P.,* and limited his privacy analysis to two considerations: whether Cutshall was entitled to the privacy interest he was attempting to assert and, if his right did exist, whether it would encompass information regarding his sex offender status. Judge Ryan first reasserted that *Whalen* did not establish a constitutional protection against disclosure. He wrote:

> [T]o support the existence of a privacy interest in avoiding publication of personal matters, the [*Whalen*] Court cited only concurring and dissenting opinions. We find no authority in that case for the proposition that such an interest exists. At any rate, the *Whalen* Court concluded that the law at issue, which compiled data on patient prescriptions, did not implicate the alleged privacy interest in avoiding the disclosure of private matters. In the same vein, we are not persuaded that the Act infringes on any constitutionally protected privacy interest.[514]

Once he established that the Sixth Circuit would not recognize Cutshall's privacy right in nondisclosure, Judge Ryan then considered whether Cutshall's sex offender status was sufficient to trigger due process protection under the Fourteenth Amendment as a protected liberty. Cutshall argued that the stigma attached to his status would harm his ability to find employment and unconstitutionally invade his right to be let alone. Judge Ryan acknowledged that Cutshall's reputation would suffer significant harm, but he relied on *Paul v. Davis* and held, "Cutshall's claim that the Act violates his Fourteenth Amendment rights because it imposes a stigma and deprives him of employment and privacy is likewise without merit."[515] He concluded that "reputation alone is not a constitutionally protected liberty or property interest."[516]

---

[514] *Id.* at 480.

[515] *Id.* at 479.

[516] *Id.* (citing Paul v. Davis, 424 U.S. 693, 701 (1976)).

§ 1983 and Qualified Immunity Cases

The second broad category of information privacy cases involves claims filed under §1983 of the Civil Rights Act,[517] which "provides a cause of action against 'any person' who, while acting 'under color of' state law, subjects or causes the plaintiff to be subjected to a violation of federal constitutional or statutory rights."[518] Often, the defendant in a §1983 case will move for summary judgment on one of two grounds: he or she is entitled to qualified immunity from liability for the infringement or the plaintiff doesn't have cause to file suit because the privacy right he or she claimed doesn't exist.[519] If qualified immunity is not granted to the defendant, the suit proceeds to trial as a civil action. The constitutional issues are typically addressed only after the court rules on qualified immunity.

Qualified immunity analysis has two steps. First, a court will establish whether the plaintiff has a privacy interest in the information at issue. Second, it will determine if the right was clearly established at the time of the alleged infringement to such an extent

[517] 42 U.S.C.A. § 1983. With its roots in the Civil Rights Act of 1871, § 1983 holds that "every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress, except that in any action brought against a judicial officer for an act or omission taken in such officer's judicial capacity, injunctive relief shall not be granted unless a declaratory decree was violated or declaratory relief was unavailable. For the purposes of this section, any Act of Congress applicable exclusively to the District of Columbia shall be considered to be a statute of the District of Columbia."

[518] Jack M. Beermann, *Symposium: Association of American Law Schools: Private Parties as Defendants in Civil Rights Litigation: Why do Plaintiffs Sue Private Parties Under Section 1983?*, 26 CARDOZO L. REV. 9 (2004).

[519] BLACK'S LAW DICTIONARY 766 (8th ed. 2004) (defining "qualified immunity" as "immunity from civil liability for a public official who is performing a discretionary function, as long as the conduct does not violate clearly established constitutional or statutory rights"); *id.* at 499 (defining a "discretionary action" as one "involving an exercise of personal judgment or conscience").

that a public official, acting in an objectively reasonable manner, would have known that his or her action(s) would infringe upon the plaintiff's right.[520]

These are not coequal stages. Resolution of these cases often depends solely upon the type of information allegedly disclosed. Courts generally review case law in order to determine whether the type of information disclosed (financial, medical, criminal, etc.) has been considered constitutionally protected in previous information privacy cases. As was the case in the statutory challenges above, the Supreme Court's holding in *Paul v. Davis* is cited frequently. Generally, the more closely related the information at issue is to the personal privacy interests traditionally protected under the Fourteenth Amendment, the more likely a court will expand privacy protections to cover that particular type of information.

Once a court has extended constitutional protection to a type of information, it must make a determination as to how well established that protection has become within the information privacy doctrine. Generally, the more frequently the courts have recognized a constitutionally protected privacy interest in a particular type of information, the more likely it is that the court will find the right "clearly established," and the less likely a defendant will be granted qualified immunity.

---

[520] *See* Harlow v. Fitzgerald, 457 U.S. 800, 818 (1982) (explaining the test for qualified immunity as "government officials performing discretionary functions generally are shielded from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known."). *See also* Anderson v. Creighton, 483 U.S. 635, 639-40 (1987) (clarifying the *Harlow* standard by providing a two-part analysis: First, "whether an official protected by qualified immunity may be held personally liable for an allegedly unlawful official action generally turns on the 'objective legal reasonableness' of the action" [as] assessed in light of the legal rules that were "clearly established" at the time it was taken (footnotes omitted), and second, "the right the official is alleged to have violated must have been 'clearly established' in a more particularized, and hence more relevant, sense: The contours of the right must be sufficiently clear that a reasonable official would understand that what he is doing violates that right").

The privacy-as-confidentiality conceptualization of privacy is recognized by the courts when the government's duty to safeguard the personal information it collects is discussed. In the substantive due process cases discussed above, the courts would review a statute, subpoena, or government-mandated information collection process to make sure it included statutory or procedural safeguards to protect personal information. However, in the following qualified immunity cases there is no explicit discussion of the government's duty to safeguard information.

In these cases, the privacy-as-confidentiality conceptualization is manifested in the denial of qualified immunity. When a court denies an individual acting under the color of law qualified immunity, it is in effect penalizing government for failing to honor its "concomitant duty" to protect personal information under *Whalen*. When a privacy right is considered clearly established, state actors have a duty to understand how their discretionary actions might infringe upon that right. Thus, in qualified immunity cases, the privacy-as-confidentiality conceptualization manifests itselfas professional conduct rather than as statutory provisions. Rather than considering whether statutory provisions are adequate to protect personal information, the court here determines whether a public official or other state actor had a "duty" to understand that his or her action violated a clearly established privacy right.

The following discussion draws upon nine U.S. Circuit Courts of Appeal cases. The first section reviews the extent to which these courts have expanded the scope of information privacy protections. Generally, privacy protections were expanded to include disclosures involving information about whether someone was pregnant, sexual escapades caught on video, sexual orientation, general medical information, HIV status,

and prescription drug use. Protections were not stretched to include court-ordered psychiatric reports, expunged plea agreements, and general financial information. The second section discusses the analytical process used by the courts to determine whether a particular privacy protection can be considered a clearly established right to privacy.

The Scope of Protected Information

The Third Circuit held that pregnancy status is constitutionally protected personal information that cannot be disclosed by a state actor absent a compelling interest. In *Gruenkw v. Seip*[521] the court recognized a privacy interest in this information because other courts have protected similar information. *Gruenke* involved a claim of qualified immunity by a swim coach at a public school who allegedly disclosed the pregnancy status of one of his swimmers, Leah Gruenke. Greunke claimed he infringed upon her right to avoid the disclosure of personal matters as framed in *Whalen*.[522]

Though Greunke's pregnancy status was a subject closely related to the fundamental interests described in *Paul,* Judge Jane Richard Roth instead considered it a form of sensitive medical information. Citing the Third Circuit's decision in *Westinghouse*, she wrote, "Gruenke's claim not only falls squarely within the contours of the recognized right of one to be free from disclosure of personal matters, but also

[521] 225 F.3d 290 (3rd Cir. 2000). Seip, a high school swimming coach, was not entitled to qualified immunity for allegedly infringing upon the privacy rights of a 17-year-old high school swimmer, Leah Gruenke. Suspecting Gruenke was pregnant, the coach pressured her to take a pregnancy test, conveyed his suspicions to other parents (not Gruenke's) as well as other students, and used Gruenke's fellow swimmers to pressure her to take a pregnancy test.

[522] *Id.* at 297. The Gruekes' claims included the following: "[T]he required pregnancy test (1) constituted an illegal search in violation of Leah's Fourth Amendment rights, (2) violated Joan and Leah's right to familial privacy, (3) violated Leah's right to privacy regarding personal matters, (4) violated Leah's right to free speech and association protected by the First Amendment, and (5) violated Joan and Leah's rights under state tort law." For purposes of this analysis, only claim #3 will be discussed as it is the only claim that implicated *Whalen*.

concerns medical information, which [the Third Circuit] previously held is entitled to this very protection."[523] Though the *Westinghouse* court never distinguished between specific types of medical information, its decision recommended that employees should have a limited right to determine which medical information is too sensitive to surrender without a compelling government interest. Judge Roth used *Westinghouse* to justify Greunke's assertion that she had a right to confidentiality in her pregnancy status. Since her coach offered no purpose for disclosure, he was denied qualified immunity.

Similarly, in 2005 the Tenth Circuit extended privacy protection to cover an individual's prescription drug usage. Judge Carlos F. Lucero wrote the opinion in *Douglas v. Dobbs*.[524] Chez Douglas was under investigation for prescription drug fraud and claimed that an assistant district attorney (Dobbs) approved a warrantless search of her prescription records byfiling a motion with a magistrate that would grant access to the records without providing "sufficient indicia of probable cause."[525]

Judge Lucero cited *Whalen* and said, "[W]e are primarily concerned . . . with the interest in avoiding disclosure of personal matters,"[526] but he held that no such privacy right had been clearly defined. He instead relied upon an earlier Tenth Circuit decision in *Herring v. Keenan*,[527] which held, "Because privacy regarding matters of health is closely

---

[523] *Id.* at 302.

[524] 419 F.3d 1097, 1100 (10th Cir. 2005). In the course of investigating Chez Douglas on suspicion of illegally obtaining prescription medication, Assistant District Attorney Pamela Dobbs allegedly "violated [Douglas'] privacy and Fourth Amendment rights by authorizing [a police officer's] submission of the Motion and proposed Order to the magistrate judge for approval to search her prescription records."

[525] *Id.* at 1102-03. Douglas was accused of using aliases to fill multiple prescriptions. Dobbs needed to access and examine her prescription drug records but at the time it was not settled law that a warrant was required.

[526] *Id.* at 1101.

[527] 218 F.3d 1171, 1173 (10th Cir. 2000).

intertwined with the activities [procreation, marriage, contraception, etc.] afforded protection by the Supreme Court. . . . 'there is a constitutional right to privacy that protects an individual from the disclosure of information concerning a person's health.'"[528] Thus, in *Douglas*, Judge Lucero held:

> Although we have not [yet] extended the "zone of privacy" to include a person's prescription records, we have no difficulty concluding that protection of a right to privacy in a person's prescription drug records, which contain intimate facts of a personal nature, is sufficiently similar to other areas already protected within the ambit of privacy.[529]

The Eleventh Circuit related the facts in its 1991 case *James v. City of Douglas*[530] to those in the Fifth Circuit's decision in *Fadjo v. Coon*.[531] The Eleventh Circuit denied qualified immunity to two police officers accused of invading a former informant's privacy when they viewed and showed to others a video tape of her having a sexual encounter with an arson suspect.[532] James was promised that the tape would be kept confidential if she would assist the police in a criminal investigation. Though the courts have often relied on *Paul v. Davis* to justify constitutional protection for intimate

---

[528] *Douglas*, 419 F.3d at 1102 (quoting 218 F.3d, at1173).

[529] *Id.* at 1102. Judge Lucero also cited the Supreme Court's decision in *Eisenstadt v. Baird*, 405 U.S. 438 (1972), when he explained, "Information contained in prescription records not only may reveal other facts about what illnesses a person has, but may reveal information relating to procreation -- whether a woman is taking fertility medication for example -- as well as information relating to contraception."

[530] 941 F.2d 1539 (11th Cir. 1991).

[531] 633 F.2d 1172 (5th Cir. 1981).

[532] Celeste James was being blackmailed by a fraud and arson suspect who had video taped them having sexual relations without her knowledge or consent. Because of this tape she was hesitant to assist police in an arson investigation, but after she was told the tape would not be shown to anyone, she agreed. The tape was eventually found during a search of the suspect's residence, and though, as promised, it was not logged as evidence, the tape was held by the police department. While it was in police custody, the tape was viewed by a number of police officers, and evidence suggests that a copy was made of the original tape.

information related to marriage, contraception, procreation, etc., the *James* court never considered the nature of the activity depicted on the tape. Instead, it relied on *Fadjo.*

The plaintiff in *Fadjo* had also surrendered personal information to investigators when subpoenaed and was promised that his information would remain confidential. After he cooperated with authorities, Fadjo's personal information was leaked to insurance investigators who suspected him of fraud. The *James* court weighed not the type of information leaked, but rather whether the investigators' promise of confidentiality created a reasonable expectation of confidentiality. Holding that the promise had created the duty to safeguard the information surrendered, the court held that there was a recognized right to confidentiality in information collected by the government following a promise not to disclose the information.

Whereas in *Greunke, Douglas*, and *James,* judges looked to other courts to determine if specific types of information should be protected within their own, a number of cases make the determination based upon the relationship between the information in question and the fundamental interests listed in *Paul*. For example, in *Sterling v. Borough of Minersville*,[533] the Third Circuit held that individuals have a privacy right to avoid having public officials threaten to disclose their sexual orientation.[534] Here the court expanded the information privacy doctrine in two ways: by holding that one's

[533] 232 F.3d. 190 (3rd Cir. 2000).

[534] *Id.* at 193. Police officers found two teenaged boys in a car behind a closed beer distributorship. It was evident to the officers that the two had been drinking alcohol, and when the boys gave sketchy answers regarding what they were doing in the car, two police officers searched the car and found condoms. Following his arrest for underage drinking, eighteen-year-old Marcus Wayman was told by a police officer that if he "did not inform his grandfather about his homosexuality that [the officer] would take it upon himself to disclose this information." As a result, Wayman told his friend that he would kill himself, and, after being released, he went home and committed suicide.

sexual orientation is protected information and also by holding that a mere "threat" of disclosure is enough to trigger constitutional protection.

Judge Carol Los Mansmann held that one's sexual orientation involves a sufficiently intimate aspect of life to qualify as a fundamental protected liberty as established in *Roe v. Wade*.[535] She noted that the Supreme Court had placed a "heavy emphasis on the intimate relationship of husband and wife in deciding that personal decisions relating to marriage are free from unjustified government interference" in *Griswold*,[536] and that later in *Eisenstadt v. Baird*[537] the Courthad held that"the right to privacy is not limited to certain relationships."[538] Judge Mansmann incorporated homosexual partnerships under the umbrella of intimate relationships protected by a constitutional right to privacy.[539]

Officials in *Sterling* had not actually revealed the individual's sexual identity but rather threatened to disclose it. The Third Circuit decided a "threat" of disclosure

---

[535] 410 U.S. 113, 152 (1973) (defining the personal privacy right as existing only in "personal rights that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty'").

[536] Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

[537] 405 U.S. 438 (1972).

[538] *Sterling*, 232 F.3d. at 194.

[539] *Id.* Judge Mansmann distinguished *Bowers* from *Whalen* by reasoning that in *Bowers* a statute criminalized "conduct" but not "status". She then held that *Bowers* "is not determinative of whether the right to privacy protects an individual from being forced to disclose his sexual orientation. In other words, the decision did not purport to punish homosexual status; *and Id.* at 196. Judge Mansmann wrote, "Wayman's sexual orientation was an intimate aspect of his personality entitled to privacy protection under *Whalen*," and "it is difficult to imagine a more private matter than one's sexuality and a less likely probability that the government would have a legitimate interest in disclosure of sexual identity." *See* Bowers v. Hardwick, 478 U.S. 186 (1986) (upholding a Georgia statute that criminalized homosexual sodomy); *see also.* Lawrence v. Texas, 539 U.S. 558 (2003) (overturning *Bowers* by striking down a Texas law that criminalized homosexual, sexual conduct reasoning that "[such] statutes do seek to control a personal relationship that, whether or not entitled to formal recognition in the law, is within the liberty of persons to choose without being punished as criminals").

constituted an infringement upon a privacy right. Judge Mansmann relied upon the confidentiality branch of privacy as framed in *Whalen* and held:

> [T]he essence of the right to privacy is in "avoiding disclosure of personal matters." The threat to breach some confidential aspect of one's life then is tantamount to a violation of the privacy right because the security of one's privacy has been compromised by the threat of disclosure. Thus, [the officer's] threat to disclose [the plaintiff's] suspected homosexuality suffices as a violation of [the plaintiff's] constitutionally protected privacy interest.[540]

Judge Mansmann's use of the word "security" indicated her understanding that a "secure state of mind" attaches to a right of confidentiality. Thus far, the Third Circuit is the only jurisdiction to recognize this interest.

Conversely, the circuit courts have also used other circuit court decisions and the Supreme Court's decision in *Paul* to justify not extending privacy protections to certain types of information. For instance, the circuits did not extend protection to include a right of confidentiality in an individual's court-ordered, psychiatric evaluations. In *Borucki v. Ryan*,[541] First Circuit Judge Herbert N. Meletz granted qualified immunity to a district attorney who had revealed the contents of such a report at a press conference.[542]

---

[540] *Sterling*, 232 F.3d. at 197.

[541] 827 F.2d 836 (1st Cir. 1987).

[542] District Attorney W. Michael Ryan ordered a psychological examination to verify that Robert Borucki was fit to stand trial. Borucki was arrested in connection with damage done to twenty-three aircraft at Northampton airport in Massachusetts. In Massachusetts the prosecution can order psychiatric evaluations not only to determine if a defendant is fit to stand trial but also to determine if the crime in question was in any way related to any psychological condition. Ryan determined that Borucki's crime was a result of his condition. Ryan eventually dismissed the criminal charges against Borucki, yet he held a press conference at which he revealed the contents of Borucki's psychiatric examination. Borucki sued for invasion of privacy under the Eighth and Fourteenth Amendments. Ryan filed a motion for summary judgment and argued he was entitled to qualified immunity.

Judge *Meletz* held that there was no clearly defined constitutional right of confidentiality to avoid the disclosure of one's psychiatric records. He reasoned that the contents of such reports did not rise to the level of the more intimate information that was closely tied to decisions relating to marriage, procreation, contraception, child-rearing, or education that the Court has recognized as fundamental and thus "protected liberties" under the Fourteenth Amendment. He also held that no such privacy interest resided in the penumbra of any specific amendment mentioned in *Griswold*.[543]

Stressing the vagueness of the privacy interest in avoiding the disclosure of personal information, he wrote:

> [I]t is not clear . . . whether, to be constitutionally protected by a right of nondisclosure, personal information must concern an area of life itself protected by either the autonomy branch of the right to privacy or by other fundamental rights or whether, to the contrary, the right of confidentiality protects a broader array of information than that implicated by the autonomy branch of the right to privacy.[544]

The Eighth Circuit held that a right to confidentiality did not attach to embarrassing information related to a failed attempt to become a police officer. In *Alexander v. Peffer*,[545] Judge Theodore McMillian held that the wife of a police union official lacked constitutional grounds to sue an aide to the Mayor of Omaha, Nebraska, for disclosing during an interview on talk radio her failed attempt to join the force.[546]

---

[543] *Griswold*, 381 U.S. at 484 (1965).
[544] *Borucki*, 827 F.2d at 841.

[545] 993 F.2d 1348 (8th Cir. 1993).

[546] *Id.* at 1349. Jane Alexander alleged that "[Walter Peffer] acting in his official capacity intentionally and deliberately publicly disclosed personal information about her in violation of her constitutional right to privacy, liberty, and property and in deprivation of her freedom of association as the wife of a union official." Alexander, a secretary in the records section of the City of Omaha Police Department, unsuccessfully tried to become a police officer. Walter Peffer then disclosed Alexander's attempt while he was being interviewed with Alexander's husband, James, a police officer and member of the Executive Board of the Police Union 101, on a radio show.

Judge McMillian cited *Paul* to establish that the Supreme Court held that a constitutional right to privacy is not intended to protect "reputation alone."[547] He held: "[T]o violate [a] constitutional right of privacy the information disclosed must be either a shocking degradation or an egregious humiliation . . . or a flagrant breech of a pledge of confidentiality which was instrumental in obtaining the personal information."[548] The reference to a failed attempt to gain employment did not rise to such a level.

The Eighth Circuit also held thatthe record of a plea agreement, even if expunged, was not protected under the right of confidentiality. In *Eagle v. Morgan*,[549] Judge Floyd R. Gibson granted qualified immunity to a City Council member who disclosed a previously expunged, criminal plea agreement at a City Council meeting and to the police officers who used national and state criminal databases[550] to locate the disclosed records.[551]

---

[547] *Id.* at 1350.

[548] *Id.* at 1350-51. He reasoned further: "The disclosures neither involved matters deemed to be fundamental rights nor addressed highly personal medical or financial information. Moreover, the statements and comments allegedly made by appellee do not constitute the type of governmental abuse that demands a constitutional response." He concluded that the "personal information disclosed on the radio show did not rise to the level necessary to be constitutionally protected" and held that "the information disclosed by [Peffer], although exhibiting poor judgment and a lack of sensitivity, implicates neither the confidentiality nor the autonomous branch of the right to privacy."

[549] 88 F.3d 620 (8th Cir. 1996).

[550] The computer databases used were the National Crime Information Center (NCIC) and the Arkansas Crime Information Center (ACIC). Eagle's records were also released to a number of reporters through the Arkansas Freedom of Information Act.

[551] *Eagle*, 88 F.3d at 623. In 1987, David Eagle, prior to becoming an auditor for the City of Jonesboro, had pled guilty to stealing building materials. Once he had successfully served his sentence and probation, his record was expunged as part of a first-time-offender program in Arkansas. Eagle had completed an audit of police salaries for the purpose of making sure personnel were being paid competitive wages, and law enforcement officers who were not happy with his findings used computer databases to locate records of Eagle's felony plea bargain. These records were forwarded to Rohnny McDaniel, who revealed Eagle's past digressions by reading from his file at the City Council meeting in an apparent effort to undermine Eagle's audit results.

Judge Gibson accepted the plaintiff's claim as one rooted in the confidentiality branch of privacy protections from *Whalen*, but wrote: "We acknowledge that the exact boundaries of this right are, to say the least, unclear . . . . [W]e discovered that courts have traditionally been reluctant to expand this branch of privacy beyond those categories of data which, by any estimation, must be considered extremely personal."[552] Further, Judge Gibson reasoned that the information in *Eagle* "seems more analogous to circumstances in which courts have refused to recognize a legitimate expectation of privacy."[553] He wrote: "Far from being 'inherently private,' the details of [the plaintiff's] prior guilty plea are by their very nature matters within the public domain. Accordingly, we decide without hesitation that Eagle has no legitimate expectation of privacy in this material."[554]

Moreover, that the plea agreement had been expunged was not found to increase its level of privacy protection. Judge Gibson reasoned:

> An expungement order does not privatize criminal activity. While it removes a particular arrest and/or conviction from an individual's criminal record, the underlying object of expungement remains public. Court records and police blotters permanently document the expunged incident, and those officials integrally involved retain knowledge of the event. An expunged arrest and/or conviction is never truly removed from the public record and thus is not entitled to privacy protection.[555]

---

[552] *Id.* at 625.

[553] *Id.* (citing circuit court privacy opinions reviewing information such as past criminal activity, official acts, false rumors, etc.).

[554] *Id.* at 625-26. Judge Gibson stressed that in accepting the plea agreement, Eagle disclosed "his transgression in an intrinsically public forum" and "acknowledged before all his fellow citizens that he had committed a crime against the laws of Arkansas . . . . He cannot now claim that a subsequent disclosure of this same information constituted a constitutional violation."

[555] *Id.* at 626.

That the court found the expunged plea agreement to still be a matter of public record also meant that the plaintiff had no privacy interest that was violated by the use of databases by public officials to locate records of the agreement. Judge Gibson stressed that the material in these particular databases was already "public" and held, "Because [there is] no legitimate expectation of privacy in the contents of [a] criminal history file, we cannot agree that the officers violated [a] constitutional right when they engaged in an unwarranted search of this material."[556]

Clearly Established Protections

The second stage of a qualified immunity case begins once a court has decided that a particular type of information warrants protection. Following such a determination, a court will then evaluate how well established the privacy protection at issue was at the time of the alleged infringement. For instance, in *James*, the Eleventh Circuit held that protection for personal information obtained by a police officer under a promise of confidentiality had been firmly established. The court relied on the Fifth Circuit's decision in *Fadjo*. Noting that *Fadjo* had been decided seven years prior to *James*,[557] the court held, "The opinion in *Fadjo* establishes the rule that a state official may not disclose intimate personal information obtained under a pledge of confidentiality unless the

[556] *Id.* at 68.

[557] James v. City of Douglas, 941 F.2d 1539, 1544 (11th Cir. 1991). The court decided to apply the precedent set in the Fifth Circuit and noted that the "court in *Fadjo,* seven years before the conduct at issue in this case, held that if the allegations contained in Fadjo's complaint were true it would amount to a constitutional violation. Therefore, *Fadjo* clearly established the constitutional right James alleges was violated by officers Purvis and Thomas."

government demonstrates a legitimate state interest in disclosure which is found to outweigh the threat to the individual's privacy interest."[558]

If a court holds that a particular privacy protection has been clearly established, then a duty to safeguard personal information attaches to the actions of the defendant(s). In making this determination, the courts embrace the privacy-as-confidentiality conceptualization. In *James*, the Eleventh Circuit framed the question before the court as "whether [the defendant's] reasonably could have believed that allowing these other individuals to view the tape was lawful in light of existing law."[559] The *James* court found that the investigators had no legitimate interest in viewing or showing the tape and "viewed the tape for their own personal gratification."[560] The privacy protections were established to the extent that the police officers, absent a compelling interest, should have been aware that their actions were violating the plaintiff's privacy interest in the tape. They were denied qualified immunity.

Similarly, in *Sterling*, the case involving the threatened disclosure of a person's sexual orientation, the Third Circuit held, "[T]he law is clearly established that matters of personal intimacy are protected from threats of disclosure by the right to privacy."[561] Judge Mansmann noted that in the Third Circuit, "A right is clearly established if its outlines are sufficiently clear that a reasonable officer would understand that his actions violate the right."[562] She concluded that disclosing a person's sexual orientation did

---

[558] *Id.*

[559] *Id.* at 1542.

[560] *Id.* at 1544.

[561] Sterling v. Borough of Minersville, 232 F.3d. 190, 192 (3rd Cir. 2000).

[562] *Id.* (citing Assaf *v. Fields,* 178 F.3d 170, 174 (3rd Cir. 1999).

qualify as an invasion of privacy under the confidentiality branch of *Whalen* and that the area of the law was sufficiently established to prevent the officers from using their qualified immunity.[563]

In *Greunke*, the case about the pregnant high school swimmer, Judge Roth held: "[T]he District Court[564] misconstrued the test for determining whether an allegedly violated right is clearly established . . . . [T]he test is not whether the current precedents protect the specific right alleged but whether the contours of current law put a reasonable defendant on notice that his conduct would infringe on the plaintiff's asserted right."[565] She held that information regarding procreation was the type of intimate information to which the Supreme Court had consistently extended privacy protections.

One court determined that the case before it dealt both with clearly established rights and vaguely defined rights. *Denius v. Dunlap*[566] was discussed above in terms of the substantive due process analysis. The case involved teachers in a government-run program for high school dropouts being forced to sign an "Authorization for Release of Personal Information" as a condition for continued employment. Though the agreement requested access to a wide variety of information, Judge Joel Martin Flaum narrowed the scope of his analysis to financial and medical information.[567]

---

[563] *Contra. Sterling*, 232 F.3d. at 200 (Stapleton, J., dissenting) (arguing that "the Court cites no case in which a threat to violate a right to privacy has been held to violate the Constitution" and that therefore the area of constitutional privacy is not well enough settled to prevent the officers from winning their motions for qualified immunity).

[564] Greunke v. Seip, 1998 U.S. Dist. WL 734700 (E.D.Pa. Oct. 21, 1998).

[565] Anderson v. Creighton, 483 U.S. 635, 639 (1987).

[566] 209 F.3d 944 (7th Cir. 2000).

[567] *Id.* at 955-56. Denius appealed claiming that the "Authorization also permits the release of other confidential information including all records pertaining to: 1) educational, 2) financial, 3)

Judge Flaum first noted that the Seventh Circuit had previously established a "substantial right in the confidentiality of medical information" in Anderson *v. Romero*[568] and therefore officials should have been "on notice that [medical] information has constitutional protection . . . and that the state cannot require its disclosure without a sufficient countervailing interest."[569] Conversely, he found that the right to confidentiality in financial information was not yet clearly established.

When deciding that protection for a particular type of personal information is not clearly established, the circuit courts have often criticized the vagueness of *Whalen* and *Nixon*. For example, in *Borucki*, Judge Meletz held that a right of confidentiality in one's psychiatric records was too vaguely conceived to constitute "clearly defined" law in 1983. He arrived at this conclusion following his review of *Whalen*, *Nixon*, and *Paul*. Judge Meletz decided that though such information was protected by the "confidentiality" branch of constitutional privacy, *Whalen* had not gone far enough to "clearly define" the constitutional right of confidentiality. He wrote, "[I]n *Whalen,* the Court reserved decision . . . on whether a duty to prevent public disclosure has roots in

---

military/veterans, 4) criminal, or 5) employment matters," but provides "no justification at this stage for requiring disclosure of this broad range of information." Judge Flaum wrote: "Denius argues that it is clearly established that the state could not require the release of confidential information without at least some interest to place in the balance and some measures limiting the use of the information and protecting it from further disclosure. Although Denius alludes in his brief to the Authorization's effect on his privacy rights in a broad range of confidential information, he only discusses with specificity his interest in medical and financial information. Therefore, we address his privacy argument with respect to these two types of information alone."

[568] 72 F.3d 518, 522 (7th Cir. 1995) (explaining that "a number of cases in the lower federal courts, including our own, building on *Whalen* and *Nixon,* recognize a qualified constitutional right to the confidentiality of medical records and medical communications . . . .(footnotes omitted) [Though it] has been expressly rejected by the Sixth Circuit . . .[i]t is recognized by our court and was in 1992."

[569] *Denius*, 209 F.3d at 956-57.

the constitution,"[570] and "*Whalen* provides very little guidance regarding the nature of the confidentiality branch of the right to privacy."[571]

Judge Meletz's review highlighted the murkiness of constitutional privacy doctrine. In granting the defendant qualified immunity, he held:

> [W]e conclude that Supreme Court cases decided prior to June 17, 1983 had not clearly established that a constitutional right of privacy would be implicated by state disclosure of the contents of a court-ordered psychiatric report. First, it was not clearly established, nor has it been argued here, that the area of psychiatric care, like 'marriage, procreation, contraception, family relationships, and child rearing and education,' is within the areas protected by the autonomy branch of the right of privacy. Second, given the predominantly fourth amendment context of *Nixon;* the uncertain import of the Court's decision in *Paul;* and the paucity of concrete guidance in *Whalen,* it was not clearly established that personal psychiatric information is information protected under the confidentiality branch of the right of privacy.[572]

In *Denius*, Judge Flaum reviewed the constitutionality of an "Authorization for Release of Personal Information" that teachers in a government-run educational program had to sign as a condition for continued employment. In his qualified immunity analysis**,** as noted above, Judge Flaum found the medical information was clearly protected. However, he noted, "[I]t is not clear whether other confidential information, such as that contained in financial records, also receives similar protection under this right."[573]

Judge Flaum reasoned, "Seven of our sister circuits have found that the constitutional right of privacy in confidential information covers some financial

---

[570] Borucki v. Ryan, 827 F.2d 836, 848, n. 19 (1st Cir. 1987).

[571] *Id.* at 841.

[572] *Id.* at 844-45.

[573] *Denius*, 209 F.3d at 956.

disclosures,"[574] but because the right to privacy in certain types of financial information was newly recognized, he ultimately concluded, "[W]e do not find that the law in this area was so clearly defined that a government official can be charged with its knowledge."[575] Thus,the defendant in *Denius* was entitled to qualified immunity in regard to medical information but not financial information.

Though Judge Flaum had found the interest in avoiding the disclosure of medical information in general to be clearly established in *Denius*, Judge Arthur L. Alarcon, writing for the Tenth Circuit in *Herring v. Keenan*,[576] held, "[T]here is a constitutional right to privacy that protects an individual from the disclosure of information concerning a person's health," but "it was not clearly established, at the time [of the defendant's] disclosure, that a probationer had a constitutionally protected right to privacy regarding information concerning his or her medical condition."[577] *Herring* involved a probation officer who disclosed to one probationer's sister and employer that he was HIV positive. Judge Alarcon considered the specific privacy interest in one's HIV status. He held that the plaintiff "failed to demonstrate that the contours of that right were sufficiently clear in late 1993 so that a reasonable probation officer would understand that he or she could not disclose to [third parties] that the probationer had tested positive to HIV."[578]

---

[574] *Id.* at 957 (citing decisions from the second, fourth, fifth, eighth, tenth, and eleventh circuits) and (noting that "the only circuit to explicitly disavow such a right, and the right of confidentiality in general, is the Sixth Circuit . . . . However, we explicitly recognized our disagreement with the Sixth Circuit's approach in *Anderson* where we agreed with the majority of circuits that *Whalen* and *Nixon* delineate a federal right of confidentiality.").

[575] *Id.* at 958.

[576] 218 F.3d 1171, 1172 (10th Cir. 2000).

[577] *Id.* at 1173.

[578] *Id.* at 1179.

In the recent Tenth Circuit case, *Douglas v. Dobbs*,[579] Judge Lucero distinguished the case involving an investigation into an individual's alleged prescription drug fraud from *Whalen* when he noted that warrants play a direct role in criminal investigations rather than serving a purely regulatory function as did the statute in *Whalen*. He then concluded, "Whether a warrant is required to conduct an investigatory search of prescription records, in contrast to the regulatory disclosures at issue in *Whalen,* is an issue that has not been settled, and is an issue we need not decide in the present case."[580] Thusthe privacy interest in prescription drug records had not been clearly established, the assistant district attorney could not be expected to know her actions were violating Douglas' rights, and, thus, her claim for qualified immunity was allowed to stand.

Conclusion

Information privacy cases generally involve either a constitutional challenge to a statute, subpoena, or other government collection of personal data or to the action(s) of a public official or other state actor. Plaintiffs claim their right to avoid the disclosure of personal matters, their right to confidentiality, has been violated. In each case the government has compelled individuals to surrender control of their personal information and thereby has assumed a duty to safeguard the information it collects. When the courts review government efforts to honor its concomitant duty to safeguard the surrendered information, the Supreme Court and the U.S. Circuit Courts of Appeal recognize a new conceptualization of privacy, privacy as confidentiality.

---

[579] 419 F.3d 1097 (10th Cir. 2005).

[580] *Id.* at 1103.

This new conceptualization differs from the privacy-as-information-control conceptualization because instead of having the right to directly control access to personal information, individuals now have a right to compel government to control access to their personal information by third parties. When a statute is challenged, this duty is honored by the inclusion of statutory provisions that safeguard the personal information that has been surrendered. In qualified immunity cases, this duty takes the form of an expectation that state actors will be familiar with clearly established information privacy interests and avoid violating individuals' privacy through their actions.

Using the vague guideposts provided by the Supreme Court in *Whalen*, *Nixon*, and *Paul*, the U.S. Circuit Courts of Appeal have slowly been shaping the information privacy doctrine. All have accepted that the right to avoid the disclosure of personal matters is either a protected liberty under the Fourteenth Amendment or an implied right with roots in the penumbras of specific protections in the Bill of Rights. All the circuit courts except the Sixth have adopted intermediate scrutiny in the form of a balancing test as the appropriate level of substantive due process review for information privacy cases.

When utilizing a balancing test, courts determine the individual privacy interest at risk by considering the type of information in question, the type of plaintiff claiming infringement, how government is safeguarding the information it collects, and the government's interest in collecting the information. A number of general trends have emerged from the circuit courts regarding these evaluations.

The more closely information is related to the fundamental interests traditionally protected in Fourteenth Amendment due process privacy cases – marriage, procreation,

contraception – the higher the level of constitutional protection is afforded. Also, plaintiff categories are forming along a continuum with private citizens having the highest level of protection, government employees a moderate level, elected public officials a lower level, and convicts the lowest level. The more protected an individual privacy interest in personal information is, the more compelling the government's justification for infringement must be in order to withstand judicialscrutiny .

A balancing test is not utilized in qualified immunity cases. In these cases the courts will look to other circuits and the Supreme Court to determine if a particular type of information has been typically protected or if the right to confidentiality should be extended to include it. If a court decides that the information in question is protected, then it must evaluate how well established the right of confidentiality in that type of information was at the time of the alleged infringement. State actors are not entitled to qualified immunity if their action(s) violated a clearly established information privacy right.

CHAPTER V

KDD AND PRIVACY

The previous three chapters have identified the primary conceptualizations of privacy as implicitly and explicitly expressed by the courts in First Amendment, Fourth Amendment, and information privacy cases. This chapter discusses whether any of the four conceptualizations identified is sufficient to protect individual privacy interests in personal information against federal utilization of KDD technology for domestic surveillance purposes. To answer this question, it is necessary to understand how KDD dataveillance is conducted.

Once the KDD process is deconstructed and explained below, this chapter concludes that though the privacy-as-information control and privacy-as-confidentiality conceptualizations may offer some privacy protections during the pre-KDD processes stage, none of the four conceptualizations afford privacy protection against the KDD applications themselves. Though the courts recognize that KDD technologies do provide a glimpse at an individual's inviolate personality, the privacy-as-space conceptualization is not directly applicable since KDD involves electronic access to databases containing digital information about many individuals rather than an intrusion into the private realm of a single person. Also, given the courts' general acceptance of the notion of limited privacy in First and Fourth Amendment privacy cases as well as in information privacy cases, the privacy-as-secrecy conceptualization is likely of little practical value to

plaintiffs. A new conceptualization of the constitutional right to privacy is necessary to protect individual information privacy interests against KDD applications.

In determining whether the use of KDD technology, which allows analysts to discover new knowledge about individuals by looking for data patterns in their digital dossiers, will infringe upon the general right to privacy or the right to information privacy in particular, it is important to understand that KDD applications are not monolithic.[581] They comprise a number of sub-processes. Any single sub-process might be challenged on constitutional grounds, and a complete analysis of possible infringements throughout an entire KDD application is beyond the scope of this study. This dissertation is focused specifically on the threat posed by the application of KDD technology to data after all of the pre-KDD processes have been completed.

The privacy-as-information-control and privacy-as-confidentiality conceptualizations, if strictly applied by the courts to the myriad methods that government utilizes to gather data and prepare searchable dossiers, provide avenues through which individuals might attempt to protect themselves against pre-KDD procedures. The actual KDD applications, however, represent a challenge to the existing privacy doctrines because they create new knowledge. Neither one's right to exert control over existing information or to compel the government to protect information it has forced individuals to surrender can protect knowledge about individuals that has been created by the government. KDD applications. Therefore, like previous new surveillance

[581] *See* Clark, *supra* note 1 (defining dataveillance); SOLOVE, *supra* note 4 (defining digital dossiers); Tether, *supra* note 5 (defining data mining); Zarsky, *supra* note 5 (quoting U.M. Fayaad, the father of data mining, defining data mining); *and* Jensen, *supra* note 9 (explaining why the term Knowledge Discovery in Databases (KDD) is the preferred term for data mining conducted for the purpose of dataveillance).

technologies, KDD technologies are now forcing the current privacy and information privacy doctrines to change once again.

Pre-KDD Data Processes

Unlike the national data center proposed in the 1960s, modern KDD technologies are decentralized. This means that rather than "collecting" data from thousands of sources and "warehousing" the data in one massive digital storage facility, the United States Intelligence Community (USIC) has concentrated on developing software solutions that will apply KDD technologies to local databases that are held, maintained, and secured at their local point of origin. This process has three stages: gathering, formatting, and sharing.

The first step in the pre-KDD process is to effectively link specific local databases to form a temporary datascape to which the actual KDD analysis can be applied. Government software "gathers" data by accessing information previously surrendered by individuals that is stored in various local databases, private and public, and then determines which records will be included in the KDD analysis. The software then "formats" the data. Records that are saved locally exist in diverse program languages and operating platforms. Formatting allows, in essence, the government software to "see" all the data as if they were written in the same language (code). Following the formatting, the data are "validated," which means redundancies, incomplete entries, etc. are removed from the records. The records are then copied in their formatted and validated form into a temporary database containing the newly gathered information that will be analyzed by the KDD applications.

The local databases accessed during these pre-KDD processes contain information that was either directly shared with private or public entities willingly by individuals in return for a specific benefit such as obtaining a driver's license, registering for veterans' benefits, or applying for a loan, or that was shared among public and private entities for secondary purposes after the information was initially gathered. It is at different points during data collection, storage, sharing, and aggregation, the pre-KDD processes, that privacy as aright to information control or confidentiality could be useful, but the running of KDD applications, the second stage of KDD dataveillance, does not even begin until all of these processes have been completed. It is during this second stage that existing privacy conceptualizations offer inadequate privacy protection.

KDD Analysis Applications

The second stage involves the actual KDD analysis applications, which take a number of different forms that can be used alone or in combination. Kim A. Taipale, founder and executive director of the Center for Advanced Studies in Science and Technology Policy, explained the three different types of knowledge discovery:

> There are three distinct applications for [KDD] in the context of domestic security: first, subject-oriented link analysis, that is, automated analysis to learn more about a particular data subject, their relationships, associations and actions; second, pattern-analysis (or data mining in the narrow sense), that is, automated analysis to develop a descriptive or predictive model based on discovered patterns; and, third, pattern-matching, that is, automated analysis using a descriptive or predictive model (whether the model itself is developed through automated analysis or not) against additional datasets to identify other related (or "like") data subjects (people, places, things, relationships, etc.).[582]

Below are simplified but accurate examples of these applications.

[582] Taipale, *supra* note 63, at 175.

Subject-oriented link analysis is used to establish links between one individual and various other persons, organizations, and activities. It is the most basic form of KDD and produces the raw material for more advanced applications. For example, if agents arrest a suspected terrorist, they might take his cell phone, credit card, and computer. Agents can then use information such as the phone numbers dialed from his phone, e-mails sent and received, credit card purchases, or Websites visited to identify his associates. KDD applications can then link to public records such as tax or criminal histories, financial records, phone records, and online accounts pertaining to these associates.

Such information can provide insight into relationships, lifestyle, and intentions. For instance, by tracking purchases made with the suspect's credit card, law enforcement can get a clear idea of his lifestyle, where he travels, and his personal finances. The suspect's records are distributed in many different databases containing information (financial, medical, commercial, educational, and criminal), but subject-oriented link analysis can "reach out" to scan the dossiers compiled during the pre-KDD stage. This KDD application essentially builds a web of relationships and activities with the suspect at the center.[583]

Pattern analysis involves searching compiled data for correlations among a pre-defined class of subjects, such as known terrorists, that reveal a pattern. For instance, running subject-oriented link analyses on a number of terrorists might reveal certain

[583] During this process, law enforcement analysts look for commonalities. For instance, if the suspect calls one person in particular on a regular basis, law enforcement officers might run a data-matching application on the credit card histories of the suspect and this person. Such an application will reveal if these two individuals travel to the same locations, buy the same things, or have the same source of funding. Each phone number, credit card number, or e-mail address is another "link" from the subject to another individual, location, database, or account. This is a valuable tool. Such relationship-mapping could theoretically result in a terror cell being uncovered.

commonalities. Examples might include traveling on student visas, receiving funds from overseas, frequent travel to symbolic sites such as the White House, taking flying lessons, or other variables that the USIC has deemed suspicious. The goal of pattern analysis is to use algorithms to assign a probability that the presence of a certain fact – perhaps traveling on an expired student visa -- indicates the likelihood of a future behavior, such as participation in a terror attack. Thus, new knowledge is revealed about an individual, which might be expressed as: There is an 80% likelihood that person X will be involved in a terror attack at some point in the future.

In federal counterterrorism efforts, this ability to predict the probability of future behavior is critical. These KDD applications are iterative, which means that the output from one application can be used as the input data for the next analysis. For instance, in the above example, a subject-oriented link analysis was run on a suspected terrorist to identify his associates, travel patterns, and purchasing behavior. By performing multiple subject-oriented link analyses on suspected or convicted terrorists, government analysts can recognize a pattern, and through analysis, assign probabilities to various predictors that might be present in dossiers. They can then build a profile for individuals who have a high probability of being active terrorists. These patterns can be used in the pattern-matching applications described below.

Pattern Matching involves running a pattern, in the form of an algorithm, against extremely large databases to identify those individuals in the data set who share the same pattern. This is the premier application for KDD technology in counterterrorism efforts. For instance, the intelligence agencies have most likely run subject-based link analysis on each of the nineteen 9-11 hijackers and built a pattern based upon commonalities in the

data of each. These patterns, possibly called "potential-terrorist," can then be run through massive international databases to see if any individuals "match" the data pattern. As KDD is an iterative process, anyone thus identified might be investigated further using a subject-based link analysis or traditional law enforcement investigation techniques. This allows the USIC and law enforcement agencies to predict which individuals within a certain datascape are most likely to be potential terrorists. Investigatory resources can then be focused on those individuals.

The State Action Obstacle

Though this dissertation evaluates constitutional privacy protections in regard to KDD applications as opposed to pre-KDD processes, there is a significant obstacle to claiming privacy protections at either stage, the state action doctrine. It will be very difficult to challenge the government's use of KDD technologies on constitutional grounds because so much of the process is conducted by private actors.

The private-sector provides database access, KDD technology, and KDD services, which confuses the state action issue. As Robert O' Harrow, Jr. commented in his recent book: "It's a simple fact that private companies can collect information about people in ways the government can't. At the same time, they can't be held accountable for their behavior or their mistakes the way government agencies can."[584] Neil Richards also warned of the government's ability to avoid its constitutional responsibilities:

> The government has also been contracting increasingly with private businesses, by acquiring databases of personal information and funding novel private-sector data collection projects. To the extent that such private collection is not state action, it allows the government, in

[584] O' HARROW, *supra* note 3, at 8-9 (2005).

> effect, to outsource surveillance beyond the scope of otherwise applicable statutory and constitutional restrictions.[585]

Thus, it could be difficult for plaintiffs to claim an invasion of privacy because the entity actually accessing, compiling, and searching an individual's personal data may not be a state actor even though the work is being done at the bequest of the government. Making that determination may be even more difficult in the current national security posture. Details regarding the relationship between USIC and private data aggregation companies are classified.

If constitutional privacy protections are to protect personal information from pre-KDD processes and KDD applications, the state action, which has been significantly narrowed during the past few decades, needs to be applied to the private data companies that are partnered with the government in KDD dataveillance programs. Currently, much of the data collection and most of the data sharing, aggregation, and mining programs are being conducted by private companies that provide such services to both private and public clientele. Individuals have no constitutional protection against KDD activities performed by private companies. Traditionally there have been two exceptions to the state action doctrine whereby the courts have held that private entities were subject to constitutional standards regarding civil rights: the entanglement exception and the public function exception.

Under the first, if the government has become sufficiently "entangled" with a private entity in performing a particular function, that private actor can be legally

[585] Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1159 (2005).

considered a state actor.[586] For instance, if a state hospital hired a private firm to handle the day-to-day operations of its facilities, then that private firm might be a state actor with regard to the policies and procedures it applies in its capacity of running a state facility. The private company could be sued under §1983 and be liable for infringement of constitutionally protected privacy rights. Under the second exception, a private entity that performs a function that has traditionally been a function of the state can at times be a state actor.[587] For instance, if a community hires a private police force to patrol and act to preserve public safety, that private security firm may be considered a state actor if it is sued for violating the civil rights of its citizens.

Currently, it would be very difficult to determine the exact extent of the involvement of private entities in federal dataveillance because such information is highly classified. If the exact role of private companies remains difficult to ascertain, it will be hard to judge whether private companies are involved to the extent that they are "entangled" with the government regarding KDD. Plaintiffs will struggle to establish state action. Moreover, though national security is a traditional government function, dataveillance, with its roots firmly in private-sector marketing applications, is not. Depending how the courts define the function of dataveillance, as either a software

---

[586] *See* Norwood v. Harrison, 413 U.S. 455 (1973) (holding that a private school was entangled because it received free textbooks from the state), Burton v. Wilmington Parking Authority, 365 U.S. 715 (1961) (holding that a restaurant who discriminated against black customers was a state actor because its location in a public parking garage sufficiently entangled it with the city), and Public Utilities Commission v. Pollak 343 U.S. 451, 462(1952) (holding that a transit authority was a state actor when it refused to stop playing loud radio programs on its cars because a Public Utilities Commission provided "regulatory supervision" to the authority, which was sufficient for the Court to decide that the authority was entangled with the commission).

[587] *See* Marsh v. Alabama, 326 U.S. 501 (1946) (holding that a private company town had infringed upon a pamphleteer's First Amendment rights when if forbid the individual to distribute the pamphlets and justifying this decision because the private town functioned like any other municipality – providing police protection, a fire department, garbage collection, etc. -- and thus for all intents and purposes was the local government)*;* Amalgamated Food Employees Union Local 590 v. Logan Valley Plaza, 391 U.S. 308 (1968), *overruled by* Hudgenson v. NLRB, 424 U.S. 507 (1976).

application or a national security procedure, it is unclear if these companies fall under the traditional public function exception. This is the crux of the state action obstacle to constitutional privacy protections from KDD dataveillance at both the pre-KDD and KDD application stages. If one's constitutional privacy rights areto protect privacy interests in personal information from KDD dataveillance, the Supreme Court needs to apply the state action doctrine to private entities used by the government for national security, intelligence, and law enforcement purposes.

Pre-KDD Processes and Constitutional Privacy Protections

The current privacy-as-information-control and privacy-as-confidentiality conceptualizations offer some protection for personal information regarding certain actions during the gathering, formatting, and sharing stages of the pre-KDD processes. The right to privacy as information control may be breached when information surrendered to the government for one purpose is used for a secondary purpose without an individual's authorization. For instance, information surrendered for the purpose of obtaining a driver's license might be sold by a state to a private data company without notification. This company, a private actor, might then combine the license information with financial and medical data it obtained from other sources and sell access to the compiled data to the USIC and law enforcement agencies.[588] It is possible that the initial act of selling personal information to the private sector is sufficient state action to invoke one's constitutional privacy protections.

[588] *See* SYKES, *supra* note 22 (describing how the government profits from the sale of public records to private entities). It should be noted that no cases could be located in which an individual sued a state for selling information surrendered for a certain purpose, like a driver's license, to marketing or data companies.

The right to privacy as confidentiality could also be breached during the pre-KDD processes. Events since the terror attacks on 9-11 such as the passage of the USA Patriot Act[589] and the release of the 9-11 Commission Report[590] have led to an increase in government-mandated information sharing among branches, agencies, and departments within the government for the purpose of improving intelligence and law enforcement capabilities. Each time the government accesses a private database for airline passenger records or student loan records, for example, for the purpose of finding threatening patterns, it is behaving in a manner similar to the New York statute at issue in *Whalen*. The government is compelling companies to disclose personal information about individuals for law enforcement purposes.

The statute in *Whalen* was held to be constitutional in part because New York was able to demonstrate that it had honored its duty under *Whalen* to safeguard that information by keeping the data in a locked vault, limiting access to the data to specific personnel, and only running the data on "offline" computers. Assuming that the courts do broaden the state action doctrine and that existing privacy protections could then be brought to bear against federal KDD dataveillance, individuals could compel government to similarly safeguard information it obtains during pre-KDD processes.

KDD and Privacy as Knowledge Control

Once again the implementation of a new surveillance technology by the government has created a need for a new conceptualization of privacy, privacy as

[589] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[590] FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT (Authorized 1st Ed., 2004) [hereinafter 9/11 COMMISSION REPORT].

knowledge control. Privacy, when it has been conceptualized as space, secrecy, information control, or confidentiality, has always concerned preexisting information. The emergence of KDD technologies has forced the consideration of how individuals might exert constitutional privacy rights not over their personal information but rather over new knowledge created by the government that happens to pertain to them.

Whereas pre-KDD processes merely gather, format, and share personal information, KDD applications utilize thatdata for the purpose of discovering new knowledge. For instance, as noted above, KDD technology allows analysts to assign a "probability of future behavior" to individuals based upon behavioral patterns found in their digital dossiers. The government, through the use of KDD, thus creates the fact[591] that a particular individual has a certain percentage chance of engaging in a certain behavior. Though this new knowledge pertains to an individual, that individual did not willingly share it with the government (negating the privacy-as-information-control conceptualization), was not compelled by the government to surrender it (negating the privacy-as-confidentiality conceptualization), and was not even aware that such knowledge existed.

Currently, the courts' privacy conceptualizations protect information and one's own knowledge, but not new knowledge that has been derived from one's personal information. An individual cannot file a privacy claim simply because the government came to "know" something about him or her by examining information available in privately held databases and public records. Dataveillance has thus created a need for a

[591] The word "fact" is used here to mean "bits of knowledge" that result when data is surveyed with KDD algorithms. Such facts are not necessarily true but are rather like values in an equation, a variable. This bit of information is attached to an individual's record following a KDD application.

new conceptualization of privacy that will allow the courts to extend constitutional privacy protections to protect knowledge created through dataveillance.

Solove explained the difference between information and knowledge in information privacy law: "Information consists of raw facts. Knowledge is information that has been sifted, sorted, and analyzed."[592] KDD technology is about discovering knowledge, not information.

A right to privacy, conceptualized as knowledge control, is justified by the ease with which the government can discover new knowledge about individuals. Thus, this new privacy conceptualization can be predicated upon a notion already accepted by the Supreme Court, practical obscurity.[593]

In *U.S. Dept. of Justice v. Reporters Committee for Freedom of the Press*,[594] the Court discussed practical obscurity in regard to criminal rap sheets that were compiled by FBI computers. The Court recognized that when personal information was widely disbursed among different government agencies and private companies, it enjoyed a certain level of privacy protection because of how difficult it would be to manually compile the distributed data. In *Reporters Committee*, the Supreme Court recognized that computer databases stripped away that protection by making it too easy to access the

[592] Solove, *supra* note 9, at 1456.

[593] Practical obscurity exists when bits of personal information have been made public at different times, in different places, to different people, but have not been compiled at one location and made available for anyone to access. Whereas the notion of limited privacy refers to one's right to share personal information with some parties and not others, practical obscurity is about one's ability to keep his or her information distributed among different entities.

[594] 489 U.S. 749 (1989).

previously distributed data.[595] The same logic might be applied to today's KDD technologies because they have made it too easy for the government to derive new knowledge and insights about individuals from previously unrelated data.

The constitutional right to privacy, conceptualized as knowledge control, would allow the courts to burden the government's creation of new knowledge. The courts must recognize that individuals are entitled to counteract the government's KDD applications by exerting a right to compel government to provide notice that the new knowledge exists, to disclose how it is being used by the government, and to provide adequate safeguards – possibly the use of encryption, pseudonymity, or sunset provisions that guarantee that the new knowledge will be destroyed after a certain amount of time – that are designed to prevent the new knowledge from leaking. A strict application of privacy as knowledge control would also allow individuals to challenge any secondary uses of the created knowledge on information privacy grounds.[596] Thus, this new conceptualization would be a hybrid of the privacy-as-information-control as originally conceived in the

[595] *Id.* at 762-64. In *Reporters Committee*, the Court considered whether rap sheets (complied criminal histories) that had been collected and stored in a central FBI database should be made available to the public under the Freedom of Information Act (FOIA). The Court recognized that Medico's criminal history was "practically obscured" until the FBI compiled it all into one location. Justice Stevens wrote: "Recognition of this attribute of a privacy interest supports the distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole. The very fact that federal funds have been spent to prepare, index, and maintain these criminal-history files demonstrates that the individual items of information in the summaries would not otherwise be 'freely available' either to the officials who have access to the underlying files or to the general public."

[596] Since KDD applications are iterative -- output from one operation is used as input for another -- newly created knowledge will likely be attached to an individual's identity and then possibly used in additional KDD applications. At this stage, the privacy-as-knowledge-control conceptualization of privacy could offer a layer of protection by allowing individuals to challenge the government's secondary usage of the discovered knowledge absent a showing of a substantial interest or particularized suspicion. The new conceptualization would allow citizens to exercise privacy as information control or privacy as confidentiality or new knowledge rather than merely preexisting personal information.

privacy scholarship and the privacy-as-confidentiality conceptualization that is now emerging from information privacy jurisprudence.

Implications for Law Enforcement's Use of KDD Dataveillance

The new privacy-as-knowledge-control conceptualization of privacy would not prohibit KDD dataveillance, but it would protect individuals by burdening the government's use of the new technology. In order to fully adopt the new conceptualization, the courts must treat dataveillance the same way they treat traditional searches in Fourth Amendment jurisprudence. They must treat dataveillance as a search conducted with technology with which the public is generally unfamiliar, and they must require the introduction of individualized suspicion into KDD applications.

Constitutionally, the courts currently treat dataveillance in much the same way they treat surveillance. The Supreme Court has held that the federal government and law enforcement personnel are free to observe what can be accessed from public vantage points. For example, in *Laird v. Tatum*[597] the Court held that the U.S. Army did not need to demonstrate probable cause prior to observing or recording demonstrators at a peace protest. Anything that could be seen or heard in public space could not be considered private. In the same way, the courts have not required a demonstration of probable cause prior to the government's accessing and using information freely given by a private entity. The instance mentioned in Chapter 1 involving JetBlue® is a good example.

Conversely, the courts grant Fourth Amendment protection to individuals when the government conducts a search. When law enforcement is looking for specific information that is not in plain sight by, for example, accessing a suspect's private papers

[597] 408 U.S. 1(1972).

or computer files, conducting DNA tests, opening locked file drawers, or looking through someone's residence or car, the Fourth Amendment mandates that the government obtain a search warrant. The most significant implication of the courts' recognition of a new privacy-as-knowledge-control conceptualization should be that the courts would begin to treat KDD dataveillance likea search rather than like traditional surveillance. This would have major due process implications for law enforcement.

Currently, dataveillance via KDD is treated more likesurveillance than a search because KDD computer software surveys information that has been previously surrendered by individuals to various public and private entities. KDD applications scan this information in the same manner a police officer might scan a crowd of protestors in an attempt to identify individuals who appear threatening in some way. The officer, conducting surveillance, would not need a warrant to observe the protesters, and if KDD applications merely scanned information, they too would not invoke constitutional protections either.

However, KDD does more than just scan information. Through the application of algorithms, KDD discovers new knowledge by searching for patterns in individual data records. This is knowledge that has not been voluntarily disclosed by individuals. Similarly, if the police officer in the example above moved beyond merely observing protestors and began searching the bags belonging to various protestors, he would need search warrants absent a compelling justification for the searches.

Moreover, under the privacy-as-knowledge-control conceptualization, the courts should recognize that KDD applications are not only similar to searches but also similar to searches conducted with new technology that is generally unfamiliar to the public. As

Justice Scalia reasoned in his majority opinion in *Kyllo*, when the public is unprepared to protect its privacy interests from a new surveillance technology, constitutional protections are necessary, and the use of new surveillance technologies should be burdened by a warrant requirement.[598] This is an additional justification for the courts to burden the government's use of KDD applications for dataveillance purposes should the privacy-as-knowledge-control conceptualization be adopted.

In adopting the new conceptualization of privacy, the courts also should address the issue of individualized suspicion. Scholars have suggested that the use of KDD technology amounts to government surveillance of millions of individuals not suspected of any crime. For instance, Dempsey and Flint argued:

> Pattern analysis raises the most serious privacy and civil liberties concerns because it involves the examination of the lawful, daily activities of millions of people. Pattern analysis poses concerns under both the constitutional presumption of innocence and the Fourth Amendment principle that the government must have individualized suspicion before it can conduct a search.[599]

The courts could answer this concern – the lack of individualized suspicion – by holding that KDD analysis becomes the equivalent of a search when the government attaches an identity to a bit of discovered knowledge. That should be the moment when an individual becomes entitled to a right to privacy as knowledge control.

A number of technological solutions have been suggested by information technology policy experts as to how law enforcement might introduce individualized

---

[598] Kyllo v. United States, 533 U.S. 27, 40 (2001). Writing for the majority, Justice Scalia held, "Where . . . the Government uses a device that is not in general public use . . . the surveillance is a 'search' and is presumptively unreasonable without a warrant."

[599] Dempsey & Flint, *supra* note 34, at 1466-67; *see also* Tien, *supra* note 30, at 405 (also arguing that an automated search of personal data is a "search" in violation of the Fourth Amendment absent particularized suspicion).

suspicion into KDD applications. As noted above, during the pre-KDD process, software reaches out and gathers data from various remote databases. At that stage, the identifying information should be encrypted and left in the localized databases from which the temporary KDD databases are initially assembled. Then the KDD applications can be run on anonymous data.

Patterns sought by the government through KDD analysis of financial, medical, educational, criminal, or other information accessed in the distributed databases are wholly recognizable without identifying information. Once analysts identify the anonymous data records that match their target pattern, the courts should then require the government to apply for a warrant prior to being permitted to reattach the identifying information to each record. Thus, the government would need to show individualized suspicion prior to beginning an investigation targeted at any one individual.

This is what Charles Weiss called Deanonymization –selective revelation of the identity of individuals connected to these patterns.[600] Weiss went on to propose a three-tiered "standard of proof" that the government should be required to demonstrate prior to reattaching the identifying information.[601] K. A. Taipale also saw Deanonymization predicated upon a showing of particularized suspicion as the solution to constitutional

[600] Weiss, *supra* note 12, at 26.

[601] *Id.* at 275-76. Weiss wrote: "[T]his article would propose that the standard of proof for Deanonymization of patterns possibly indicative of terrorist activity have three tiers. The first standard should be reasonable, articulatable suspicion—the Fourth Amendment standard for the *Terry* stop. It should apply to transaction patterns, thought to be associated with the most serious forms of terrorist activity, such as nuclear, biological, or large scale chemical attacks. The second standard should be reasonable indication, the criterion for initiating an FBI investigation. It should apply to those transaction patterns which do not point to the most serious forms of terrorist activity and are not derived from the most sensitive data or databases. The third standard should be probable cause, the Fourth Amendment standard for search, seizure, and arrest. It would apply in cases of transaction patterns not associated with these most serious terrorist activities, but relying on the most sensitive data or databases—for example, those holding personal information on finances, medical conditions, and intellectual and political activities through an individual's library books, video rentals, magazine subscriptions, Internet surfing and the like."

problems that arise from federal dataveillance. Taipale wrote, "[S]elective revelation can reduce the non-particularized suspicion problem, by requiring an articulated particularized suspicion and intervention of a judicial procedure before identity is revealed."[602] Should the courts adopt the privacy-as-knowledge-control conceptualization, the major implication for law enforcement agencies conducting dataveillance should be that prior to Deanonymization individualized suspicion will need to be demonstrated before beginning an investigation of any individual flagged by a KDD application.

Conclusion

KDD dataveillance occurs in two stages. First, during the pre -KDD processes, data are gathered from remote databases, formatted, and shared to create a temporary database to which the KDD applications can be applied. Second, KDD applications in the form of subject-oriented link analysis, pattern analysis, and pattern matching are applied to the prepared data. This second stage discovers new knowledge about individuals.

One serious obstacle to claiming constitutional privacy protections from either stage of KDD dataveillance is the heavy involvement of the private sector. Private companies involved in federal dataveillance supply data, technology, and services and cannot be held constitutionally liable for infringing upon privacy rights. The country's

[602] Taipale, *supra* note 20, at ¶29; *see also* Taipale, *supra* note 63, at 129 (discussing his proposal that "technical development strategies premised on separating *knowledge of behavior* from *knowledge of identity* based on the *anonymization* of data (for data sharing, matching and analysis technologies) and the *pseudonymization* of identity or authorization (for identification and collection technologies) can help protect individual autonomy while still meeting security needs"); *id.*at 217 (asserting that disaggregating privacy into identity and behavior for analytic purposes, and designing technical systems to help manage the circumstances of attribution, can help achieve a practical resolution to the apparent conflict between privacy-security interests).

current national security posture makes it even more difficult because information regarding the specific roles performed by private as opposed to public entities in dataveillance is classified. The existence of any constitutional protection against federal dataveillance depends upon an application of the current state action doctrine. Private data companies working with the USIC or law enforcement in dataveillance programs would need to be considered state actors under the entanglement or public function exceptions.

Assuming the state action doctrine is applied, the current privacy and information privacy doctrines, based upon conceptualizations of privacy as information control and privacy as confidentiality, if strictly applied by the courts, offer constitutional privacy protection from various pre-KDD processes. They are not, however, able to protect individual privacy interests against federal dataveillance programs using KDD applications because these applications discover new knowledge and plaintiffs are currently unable to claim a privacy interest in information that they did not actually surrender to the government.

This is another circumstance in which the development of new surveillance technology is driving the creation of a new privacy conceptualization. In order to protect individual privacy interests, the courts must recognize a new conceptualization of privacy, privacy as knowledge control. This conceptualization will allow individuals to claim privacy protection for newly discovered knowledge. As a hybrid of the privacy-as-information-control and privacy-as-confidentiality conceptualizations, the new conceptualization might allow individuals to limit the government's use of the discovered knowledge to the purpose of the specific search in which it was created as well as

empower individuals to compel government to notify individuals when information about them is created, that it is being stored for future use, and of the safeguards the government has implemented to protect the new knowledge.

If the privacy-as-knowledge-control conceptualization were adopted, there would be due process implications for the USIC and law enforcement. Currently, the courts treat dataveillance more likesurveillance than like a search. Searches require due process in the form of particularized suspicion and a warrant. Surveillance is generally unburdened by such requirements. Should the courts extend constitutional protection to KDD applications, dataveillance should be burdened by procedural due process too.

Information technology policy scholars are suggesting that particularized suspicion and a warrant be required before the government can attach an identity to otherwise anonymous data. The easiest way to accomplish this is to prohibit access to identifying information in the distributed database(s) to be used in a KDD analysis. Once a KDD application has been run on compiled but anonymous data, the USIC or law enforcement agency involved would need to apply for a warrant prior to deanonymizing the records of interest.

CHAPTER VI

CONCLUSION

The purpose of this dissertation has been to explore whether the current conceptualizations of the constitutional rights to privacy in general and information privacy in particular are adequate to protect citizens against the U.S. government's use of KDD technologies in dataveillance programs. The preceding discussion of First Amendment, Fourth Amendment, and information privacy cases has revealed the courts' current conceptualizations of privacy in those three doctrines. Chapter 5 detailed how KDD dataveillance operates and discussed why a new conceptualization of privacy is needed to protect knowledge discovered by KDD applications. This chapter reviews all five conceptualizations, presents a summary of this project's findings, and provides suggestions for further studies related to this topic.

Privacy Conceptualizations

Altogether, this dissertation has discussed five conceptualizations of the constitutional right to privacy. Three broad conceptualizations emerged from the review of scholarly literature in Chapter 1: privacy as space, privacy as secrecy, and privacy as information control. Evidence of the courts' adoption of these conceptualizations, implicit and explicit, was sought in a review of First Amendment, Fourth Amendment, and information privacy cases. A fourth privacy conceptualization, privacy as

confidentiality, was discovered in the U.S. Circuit Courts of Appeal information privacy cases. Lastly, a new conceptualization of privacy, privacy as knowledge control, was suggested in Chapter 5 as a necessary answer to the particular challenge to constitutional privacy protections posed by KDD applications.

The privacy-as-space is the oldest conceptualization of privacy with its roots in the Framers' desire to protect private property against intrusions by the federal government. Over time, this conceptualization evolved to include protections against government access to one's inner space, self, or inviolate personality as well as to physical space. The courts continue to recognize both variants of the privacy-as-space conceptualization in privacy jurisprudence.

In the mid-twentieth century America became a credentialed society, and during this period the privacy-as-secrecy conceptualization emerged. Under this conceptualization, when individuals shared information for any reason, with any third party, they surrendered their privacy interest in that information. This third-party doctrine severely limited information privacy rights because it was very difficult for one to conceal personal information and still function in society. In mid-to-late Twentieth Century, the courts began to recognize the notion of limited privacy, which held that individuals had the right to share personal information with some entities and not others.

Though the courts never explicitly rejected the privacy-as-secrecy conceptualization, it lost its practical value to plaintiffs because the courts understand that nobody can live and function in modern society without sharing personal information with various entities. Nevertheless, often during the process ofestablishing the appropriate level of protection to which specific information may be entitled, the courts

will still discuss the extent to which the information in question had been shared with others.

When the courts recognized limited privacy, they simultaneously recognized the right of individuals to choose who could access their personal information and who could not. This spawned the privacy-as-information-control conceptualization. Under, this conceptualization or its variations, privacy-as-property or privacy-as-contract, the law functioned to empower individuals relative to the publicentities that collected their personal information. One important market failure critique of privacy as information control has been that it presupposes that individuals have both the desire and technological expertise to exercise control over their personal information.

In circumstances in which the government is using surveillance technologies that are generally unknown to the public, individuals are no longer capable of protecting their individual privacy interests; thus the law must burden the government's use of such technology by conditioning their use on due process. In *Kyllo*, Justice Scalia held that searches conducted with a "device . . . not in general public use" are unreasonable without a warrant.[603] The warrant requirement is a legal limitation that compensates for new technology.

A fourth conceptualization of privacy has emerged in the new information privacy doctrine, the privacy-as-confidentiality conceptualization. It has its roots in Justice Steven's assertion in *Whalen* that "the right to collect and use [data] for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid

[603] Kyllo v. United States, 533 U.S. 27, 40 (2001).

unwarranted disclosures."[604] Under this conceptualization of privacy individuals have a constitutional right to expect the government to have statutory or procedural safeguards in place to protect the confidentiality of personal information they surrender to the government. This conceptualization also provides that state actors will be aware of clearly established privacy interests and make every effort not to infringe upon those privacy interests through their discretionary actions.

Privacy Conceptualizations in Privacy Jurisprudence

Four research questions were presented in Chapter 1. This section draws upon the case analyses in Chapters 2, 3, and 4, as well as the discussion of KDD dataveillance presented in Chapter 5 to answer each of the four questions.

RQ1: How has the U.S. Supreme Court conceptualized the constitutional right to privacy in general in First and Fourth Amendment privacy jurisprudence?

First Amendment Privacy

The First Amendment privacy doctrine is primarily concerned with identity or one's ability to speak or associate anonymously. Anonymity is the state wherein one decides to keep one's identifying information – name, address, telephone number, social security number, etc. – secret even if other aspects of his or her personality, such as political or religious affiliation, have already been disclosed. This notion of sharing only some aspects of one's identity and not others is referred to as limited privacy, and the Courts have supported this idea as central to the right to speak or associate anonymously.

[604] Whalen v. Roe, 429 U.S. 589, 605 (1977).

In Chapter 2, Supreme Court cases dealing with anonymous speech, anonymous association, and surveillance of public assemblies were reviewed. In a series of anonymous pamphleteering cases, the Court recognized the privacy-as-access-to-self conceptualization in its discussion of the importance of protecting one's most private thoughts and beliefs, his or her inviolate personality. It reasoned that when individuals choose to hand out leaflets or proceed door-to-door to collect signatures, they are associating themselves with a cause, movement, organization, or belief. The Court reasoned that materials such as political pamphlets, petitions, and religious leaflets all express political or philosophical positions and are generally intended to be persuasive. The mere act of distributing these materials in person provides strangers a glimpse of least one of the pamphleteer's or canvasser's deeply held faiths or beliefs.

An anonymous pamphleteer is an indistinct representative of a larger, more abstract belief system, but once an identity is attached to those beliefs, a more intimate portrait of the individual emerges. Individuals may choose not to participate in this form of public discourse if the cost is revealing their innermost selves to random members of the public. In this circumstance, First Amendment free expression rights have been chilled and the number of voices in the marketplace of ideas lessened. In limiting the government's ability to compel disclosure of identifying information absent a compelling state interest, the Court has protected free expression rights by empowering individuals to control the dissemination of their identifying information in First Amendment contexts.

Aside from protecting intangible interests like one's innermost thoughts and emotions, the right to control identifying information also has a more tangible benefit. Were government permitted to compel individuals to surrender their anonymity, it would

make them vulnerable to retaliation. Even if government did nothing to retaliate against those espousing unpopular beliefs, compelled disclosure of identity could indirectly enable private actors to retaliate socially, economically, or physically. The risk of retaliation, as was shown in a number of the cases discussed in Chapter 2, has proved sufficient to chill expressive behavior. The Court has recognized that privacy, conceived of as the control of identifying information, reduces the threat to intangible and tangible personal interests alike. Thus, this right to control the flow of identifying information, to choose anonymity, has been treated as an implied right under the First Amendment, necessary to the exercise of the other enumerated rights under the Amendment.

The Court's discussion regarding canvassers who go door-to-door included consideration of the right of homeowners to know the identity of the individuals who enter upon their property. This created a need to reconcile the spatial privacy conceptualization with privacy as a right to control one's own personal information. The Court concluded, generally, that property owners could not compel canvassers to disclose their identities, but they had the right "not to listen" or "not to respond" to canvassers' calls. Stated another way, property owners had a right to restrict the flow of information into their property. Thus, the spatial conceptualization was reinterpreted as a right to control information. Homeowners maintain the right to control which ideas and what information flow into their homes. At the same time, canvassers and pamphleteers maintained control over the revelation of their identities. Thus privacy as access to self was also reinterpreted as right to control information.

The First Amendment also protects the right to remain anonymous in regard to one's associations. The Supreme Court has struck down laws designed to force groups to

turn over membership lists, and it has held that it is unconstitutional for the government to directly compel – for instance in legislative hearing – individuals to disclose their own membership in particular groups or to reveal the identities of other group members. When one joins a group, in most cases the other members are aware of his or her identity. Yet the Supreme Court has protected the right of individuals to withhold the fact of their membership in groups from government. This is limited privacy, and as such, a direct refutation of the privacy-as-secrecy conceptualization.

The Court has held that groups are entitled to maintain the anonymity of their members by controlling the identifying information of their members. Again the Court recognized limited privacy. Individuals have a right to share their personal information with some entities and yet maintain a privacy interest in that same information with regard to other third parties. This is the same posture assumed by the Court in the anonymous speech cases involving pamphleteers and canvassers.

The Supreme Court also sought to prevent any chill on association rights that might result from the forcible surrender of membership information. As noted above, when individuals' identities are known, they may perceive themselves to be at risk of suffering retaliatory harms. In situations in which an individual is being compelled to disclose the identities of other members of a group, he or she may fear that all the members in the group are being exposed to the risk of retaliatory harms. If individuals believe there is a possibility they will be forced to reveal information about their groups' memberships, they may stop joining groups. This could effectively eliminate any political power certain groups might amass. Implicit in these anonymous association decisions was the notion that individuals, or groups on their behalf, should have the right to

determine their own level of exposure to risk; thegovernment should not have the power to do that for them.

Fourth Amendment Privacy

The Supreme Court's conceptualization of privacy under the Fourth Amendment has evolved through four separate stages: the Fourth Amendment as a procedural component of Fifth Amendment protections against self-incrimination, privacy as space, privacy as secrecy, and privacy as information control. The advent of new surveillance technologies has been responsible for the Court having to move through the later three stages.

During the first stage, Fourth Amendment protections were subsumed under the Fifth Amendment's protection against self-incrimination. The Framers had been wary of centralized government and sought to limit its power over individuals. They were particularly concerned about government intrusions upon private property for the purpose of obtaining material evidence to be used against individuals in Court. Fourth and Fifth Amendment analysis was combined such that material evidence gathered without a warrant was ruled inadmissible in court as a violation of the defendant's Fifth Amendment rights. This tendency to combine Fourth and Fifth Amendment protections was exemplified in *Boyd v. United States*.[605]

The Court eventually established Fourth Amendment analysis as distinct from Fifth Amendment analysis. It was the advent of a new surveillance technology, wire

[605] 116 U.S. 616 (1886).

taps, that reframed the Court's discussion in *Olmstead v. United States*[606] as one concerned with privacy as space. By tapping phone lines leading into a private space, law enforcement agents could learn what was transpiring behind closed doors without ever setting foot on private property. They could constitutionally collect personal information from within private space without a warrant.

Thus the Courtex plicitly conceptualized privacy asthe right to protect private space. No warrant was necessary to gather evidence by any means that did not require physical trespass. Court decisions during this period were generally limited to making a determination as to whether the government had procured a warrant prior to invading any private space absent consent or expedient evidentiary concerns.

In 1967 the Court adopted the privacy-as-secrecy conceptualization. It rejected the principle of limited privacy and instead embraced the third-party doctrine. This period began with *Katz v. United States*,[607] in which the Court recognized the role of personal agency in the creation of a subjectively reasonable expectation of privacy. It is tempting to think that privacy protections were expanded under such a conceptualization since it effectively made privacy portable. Constitutionally protected privacy could exist anywhere as long as one protected the information and didn't share it with third parties. For example, in *Katz*, the Court had reasoned that the plaintiff had a reasonable expectation of privacy in a public phone booth because he closed the door and paid for the exclusive use of a telephone line.

The courts would be tasked with determining whether an individual had taken sufficient action to create a subjective expectation of privacy in certain information,

[606] 277 U.S. 438 (1928).

[607] Katz v. U.S., 389 U.S. 347 (1967).

materials, or space that society in general would consider reasonable. However, in practice, this conceptualization severely limited privacy protections because the Supreme Court was very conservative regarding what constituted a reasonable expectation of privacy. If the information in question was in any way shared with a third party, then it was no longer entitled to constitutional protection. As a result, none of the information shared with banks, phone companies, or even information that might be discerned from the contents of one's garbage has been covered by the constitutional right to privacy.

The courts have now largely replaced the privacy-as-secrecy conceptualization with a new conceptualization of privacy, privacy as information control. In *Kyllo v. United States*,[608] the Court recognized that new surveillance technologies were eroding the ability of individuals to create a subjectively reasonable expectation of privacy in spaces and information. In response, the Court explicitly recognized a heightened privacy interest in situations wherein the government uses surveillance technology that is generally unfamiliar to the public. In *Kyllo* the Court implicitly held that the Fourth Amendment does not protect space so much as it protects government knowledge of what transpires within a particular space. Fourth Amendment privacy jurisprudence may become all about an individual's right to control access to personal information.

Reconciling Conceptualizations

Currently, the primary conceptualization of the constitutionally protected right to privacy in both First Amendment and Fourth Amendment privacy jurisprudence is privacy as information control. The Court never explicitly adopted nor rejected any one privacy conceptualization. Instead, it gradually began to discuss privacy interests –

[608] Kyllo v. United States, 533 U.S. 27 (2001).

anonymity, protecting one's papers in a home, protecting one's innermost beliefs, protecting the solitude of a home – in terms of information flow. Privacy as space, both physical and the self, is still discussed by the courts when evaluating privacy interests, and the privacy-as-secrecy conceptualization has been abandoned.

*RQ2***:** How have the U.S. Supreme Court and U.S. Circuit Courts of Appeal conceptualized the constitutional right to information privacy?

Information Privacy

The Supreme Court has recognized in very board terms a constitutionally protected privacy interest in avoiding the "disclosure of personal matters" [609] The source of this right has been only vaguely defined. It is at once a personal liberty under the Fourteenth Amendment Due Process Clause and rooted in the penumbras and emanations of specific protections within the Bill of Rights. The Supreme Court in *Nixon v. Administrator of General Services*[610] reaffirmed the Court's holding in *Whalen* and established intermediate scrutiny, in the form of a balancing test, as the appropriate level of judicial review in information privacy cases. The Court has also indicated that information that is more closely related to intimate choices such as marriage, procreation, and contraception is entitled to more privacy protection.[611]

This has been the extent of the guidance provided by the Supreme Court. Since *Whalen* and *Nixon*, the U.S. Courts of Appeal have been defining the scope of this right,

[609] Whalen v. Roe, 429 U.S. 589, 598-600 (1977).

[610] 433 U.S. 425 (1977).

[611] Paul v. Davis, 424 U.S. 693, 713 (1976).

labeled by the circuit courts since the Fifth Circuit's decision in *Plant v. Gonzales*[612] the right of confidentiality. In doing so, the circuit courts have collectively constructed a new conceptualization of constitutionally protected privacy, privacy as confidentiality. Under this conceptualization of privacy, individuals have the right to compel what the Supreme Court has termed a "concomitant duty" from government.[613] To fulfill this duty the government must take measures designed to safeguard the personal information that it has compelled individuals to surrender.

The privacy-as-confidentiality conceptualization differs from the privacy-as-information-control conceptualization in terms of agency. In the privacy-as-information-control conceptualization, the courts applied privacy law to enable individuals to control access to and the use of their personal information. For example, the constitutional right to privacy might prevent a city ordinance from forcing a pamphleteer to reveal his or her identity. Under the newer privacy-as-confidentiality conceptualization, the responsibility for safeguarding that information has transferred to the government.

When a statute is challenged on information privacy grounds, the court will consider whether the government has statutory or procedural safeguards in place that are appropriate to the circumstances of the challenge. In qualified immunity cases, this duty takes the form of an expectation that state actors will be familiar with clearly established information privacy law and avoid violating individuals' privacy through their discretionary actions. If a state actor violates this expectation, he or she can be sued in a §1983 civil suit.

---

[612] Plante v. Gonzales, 575 F.2d. 1119 (5th Cir. 1978).

[613] *Whalen*, 429 U.S. at 605.

Using the vague guideposts provided by the Supreme Court in *Whalen*, *Nixon*, and *Paul*, the federal circuit courts of appeal have generally recognized that the right to avoid the disclosure of personal matters by the government, the right to confidentiality, is either a protected liberty under the Fourteenth Amendment or an implied right with roots in the penumbras of specific protections in the Bill of Rights. All the circuit courts except the Sixth have adopted intermediate scrutiny, in the form of a balancing test, as the appropriate level of substantive due process review for information privacy cases.

The scope of the information privacy doctrine has been developing as the circuit courts balance individual privacy interests against the government's interest in collecting personal information. Two general types of circuit court decisions were reviewed in Chapter Four, those involving a constitutional challenge to a statute, subpoena, or other government policy and those involving a challenge to the action(s) of a public official or other state actor. In statutory challenges the court must first define the individual privacy interest at risk by considering three factors: the type of information in question, the type of plaintiff claiming infringement, and how government is safeguarding the information it collects. The privacy interest, once defined, is then weighed against the government's interest in collecting the information. This process of determining the individual privacy interest in a particular case has resulted in the emergence of a number of general trends.

Under the first factor, not all information is weighted equally in the eyes of the courts. Information related to the fundamental interests traditionally protected in Fourteenth Amendment due process privacy cases -- marriage, procreation, contraception, etc. -- will receive a higher level of constitutional protection. For instance, instead of treating "medical information" as a monolithic construct, the circuit courts

have afforded different levels of protection to different types of medical information. For example, pregnancy and HIV status have received stronger constitutional protections than prescription drug records.

Plaintiff categories have also formed along a continuum. In a hierarchy that in some ways mirrors the plaintiff categories in defamation law, private citizens have the highest level of protection, government employees have a moderate level, elected public officials have an even lower level, and convicts have the least protection. For example, the courts have held that since candidates for political office and city employees are paid with tax dollars and function in the public interest, citizens have a right to know more about them in order to deter corruption, conflicts of interest, etc. The courts have held that state and local statutes compelling political candidates, city employees, and federal employees to disclose personal financial records were constitutional. Likewise, public safety has been held to justify disclosure provisions in sex offender registry statutes in two states. Conversely, in two circuit decisions, law enforcement officials conducting criminal investigations were denied qualified immunity for breaching a promise of confidentiality to one private citizen who had been asked to aid in a criminal investigation and to another who had been subpoenaed to cooperate.

The last factor used in defining an individual privacy interest in information privacy cases is whether and how the government fulfilled its duty to safeguard the information it had compelled from individuals. Courts have considered both statutory and procedural measures. The more substantial the government's information safeguards, the weaker the individual privacy interest that can be claimed. A statute containing specific guidelines regarding how the government body will access, store, and protect personal

information is much more likely to be found constitutional. For instance, the circuit courts have accepted coding systems, locked storage rooms, limited access by government employees, and processing sensitive data on "offline" computers as adequate safeguards. The level of specificity required by the courts will vary from jurisdiction to jurisdiction. While some have required an accounting of precisely how the government would protect information, others simply verified that some form of safeguard was in place.

Consideration of the type of information at issue, the plaintiff category, and the government's information safeguards provides the court with a "value" for the individual privacy interest at stake in a particular case. The more fundamental the value is, then the more compelling the government's purpose for the alleged infringement must be. Improving the electoral process; informing citizens to enable self-government; promoting the public's general health, safety, and welfare; and national security have each been considered substantial or compelling government interests. Conversely, in the circuit cases reviewed in Chapter 4, no government interest was put forth to justify the disclosure of personal information obtained from an investigatory subpoena to an insurance investigator, for the release of sensitive commercial information disclosed during the discovery phase of a defamation trial but not used in the trial, for disclosing the pregnancy status of a high school swimmer, nor for forcing teachers in a government educational program to sign an information disclosure agreement. In each case the government's statute or action was held to be unconstitutional.

Once both the individual privacy interest and the government interest in disclosure have been defined, courts determine which is greater. If the government's

interest is greater, the legislation in question will likely be ruled constitutional. If the individual privacy interest is found to be more substantial, the legislation will likely be struck down. In Chapter 4 a two-part algebraic expression was proposed to express the relationships between factors considered by the courts in information privacy cases:

(*Type of Information* + *Plaintiff Category*) – *Government Safeguards* = *Individual Privacy Interest*

Individual Privacy Interest (>,<) *Government Interest in Information* = Decision

Resolution of a qualified immunity case does not involve a balancing test. The objective in these cases is to determine whether a particular type of information has been generally granted constitutional protection by the courts, and if not, to decide whether the right to confidentiality should be extended to include it. Should a court decide that the information in question is protected, analysis then turns to an evaluation of how clearly established a right of confidentiality in that type of information was at the time of the alleged infringement.

The test for what constitutes a clearly established doctrine varies from circuit to circuit as judicial review in the cases involves an in-depth analysis of cases from both within and without each jurisdiction that have dealt with the information in question. If at the time of the infringement there has been a Supreme Court ruling regarding the privacy interest or a number of circuit court decisions on point, then the law is more likely to be considered clearly established. The government's concomitant duty is honored in these cases if the defendant, a state actor of some kind, is aware of clearly established privacy laws and avoids infringing upon information privacy rights through his or her discretionary actions. If the defendant infringes upon the privacy of information that is protected but the legal protection is not clearly established, then the defendant is

entitled to qualified immunity and cannot be found civilly liable for the alleged infringement. State actors are not entitled to qualified immunity if their action(s) violate a clearly established information privacy right.

Privacy Conceptualizations and KDD

There are two factors that must be understood prior to a discussion of whether the courts' current conceptualizations of privacy are sufficient to protect individual privacy interests in personal information. First, KDD dataveillance is not a monolithic operation, but instead has two distinct stages, pre-KDD processes and KDD applications, and each of these has a number of sub-processes. During the pre-KDD processes, data is gathered from remote databases, formatted, and shared to create a temporary database to which the KDD applications can be applied. The KDD applications -- subject-oriented link analysis, pattern analysis, and pattern matching -- are applied to the prepared data for the purpose of discovering new knowledge. The first stage involves the manipulation of preexisting data while the second involves the creation of completely new knowledge about individuals.

Second, any constitutional protection against federal dataveillance at either the pre-KDD processes stage or the KDD applications stage will require the courts to apply the state action doctrine. Private entities are heavily involved in KDD as suppliers of data, technology, and KDD services. Individuals cannot claim an infringement upon a constitutional right against private entities. Thus, the following discussion of the adequacy of constitutional privacy protections regarding KDD dataveillance must be predicated upon the understanding that the judiciary will need to find that private entities

partnering with the USIC and law enforcement in KDD dataveillance programs are state actors under either the entanglement or public function exceptions to the state action doctrine. Absent such a holding, it is unlikely that the courts will recognize a constitutional privacy interest in personal information subjected to KDD analysis.

RQ3: What are the strengths and weaknesses of the current conceptualizations of the constitutional right of privacy in general or the constitutional right of information privacy in particular as protection against KDD?

As discussed in Chapter 5, this dissertation is concerned with the KDD analysis stage and not with the pre-KDD processes stage. If the state action obstacle was surmounted, the current conceptualizations of privacy and information privacy, if strictly applied by the courts, would offer constitutional protection from pre-KDD processes. However, the current conceptualizations of privacy are insufficient to protect individual privacy interests against federal dataveillance programs using KDD applications.

The current privacy conceptualizations fail to provide protection against KDD analysis for two reasons. First, KDD analysis applications generate new knowledge, and it is unlikely that plaintiffs would be able to claim constitutional privacy protections for information they have not actually surrendered to the government. Second, dataveillance is currently treated by the courts more like surveillance than like a search. As such, law enforcement is not burdened by a warrant requirement or even a need to show particularized suspicion.

RQ4: If a conceptualization more protective of information privacy is needed, what should it be? How might KDD applications and policies be designed to better comply with the individual constitutional right to avoid the disclosure of personal matters?

The advent of KDD dataveillance is the most recent circumstance in which the development of a new surveillance technology is driving the creation of a new privacy conceptualization. In order to protect individual privacy interests, the courts must think about privacy in a new way. They must recognize privacy as the ability of individuals to exert control over knowledge rather than merely over information. This privacy-as-knowledge-control conceptualization, a hybrid of the privacy-as-information-control and privacy-as-confidentiality conceptualizations, would allow individuals to limit the government's use of the knowledge discovered in the KDD applications to the specific purpose of the search in which it was created. It would also empower individuals to compel government to notify individuals when knowledge about them is created, that it is being stored for future use, and of the safeguards the government has in place to protect the new knowledge.

If the privacy-as-knowledge-control conceptualization were adopted, there would be due process implications for the USIC and law enforcement. Currently, the courts treat dataveillance more like surveillance than like a search. Searches require due process in the form of individualized suspicion and a warrant. Surveillance is generally unburdened by such requirements. If the courts extend constitutional protection to knowledge discovered in KDD applications, then federal dataveillance will also be burdened by procedural due process.

The exact nature of this due process requirement is yet to be determined, but information technology policy scholars are suggesting that individualized suspicion and a warrant be required before the government can attach an identity to otherwise anonymous

data. This can be accomplished by using encryption software to remove identifying information from the distributed database records being gathered for use in KDD analysis. KDD applications can then be run on compiled but anonymous data. Once analysts identify the records that match the pattern being linked, analyzed, or matched, the government should be compelled to apply for a warrant prior to deanonymizing the records of interest.

Directions for Further Study

The constitutional information privacy doctrine is still taking shape in the circuit courts. As noted above, different types of personal information receive differing levels of constitutional protection. The strongest protection is being granted to information most closely related to fundamental, personal liberties traditionally protected in decisional privacy cases – marriage, procreation, contraception, intimate relationships, etc. One interesting avenue of inquiry would be to explore whether the distinction made in *Whalen* between the privacy interest in avoiding the disclosure of personal matters and the interest in the ability to make important decisions without interference from the government is being blurred by this trend. As courts continue to grant greater protection to information related to those liberties commonly discussed in decisional privacy cases and lesser protection to unrelated information, the question will become whether information privacy is being subsumed into decisional privacy? A study looking at the language of the courts to identify evidence of such a merger would be valuable.

It would also be valuable to further define the plaintiff categories emerging in information privacy cases. The fact that categories roughly mirroring those in

defamation law are emerging from the circuit courts was briefly touched upon in this dissertation. However, a closer examination of the courts' language in these cases would likely yield a philosophical underpinning for this emerging pattern. Having a clear understanding of the courts reasoning could make this nascent doctrine more predictable across jurisdictions.

A thorough study of how KDD technology partnerships between private data companies and the USIC might justify the application of the state action doctrine by the courts would be a valuable contribution. In order to determine whether private entities involved with federal dataveillance should be included under the entanglement or public function exception, the exact nature of these national security partnerships will need to be defined. Such a project would be challenging since many of the details of these partnerships are classified because of the nation's current national defense posture. Nevertheless, a determination needs to be made as to whether the government is merely privatizing dataveillance or if it is avoiding its constitutional obligations to safeguard individual privacy interests by acting through private entities.

Another area that needs to be explored from a constitutional perspective is the value-sensitive design of new data technologies. This is exemplified above in the discussion of a process through which identifying information can be removed from digital data records prior to the application of KDD processes and then reattached to specific files only upon a showing of particularized suspicion. Technology policy experts are suggesting that privacy and national security interests can be balanced through technology implementation strategies designed to promote rather than erode constitutional values. It would be a fruitful avenue of inquiry to analyze each proposed

information technology policy in terms of the five privacy conceptualizations discussed in this dissertation.

REFERENCES

Primary Sources

Cases

U.S. Supreme Court

Amalgamated Food Employees Union Local 590 v. Logan Valley Plaza, 391 U.S. 308 (1968).

Anderson v. Creighton, 483 U.S. 635 (1987).

Barenblatt v. United States, 360 U.S. 109 (1959).

Bates v. Little Rock, 361 U.S. 516 (1960).

Bowers v. Hardwick, 478 U.S. 186 (1986).

Buckley v. American Constitutional Law Foundation, 525 U.S.182 (1999).

Buckley v. Valeo, 424 U.S. 1(1976).

Burton v. Wilmington Parking Authority, 365 U.S. 715 (1961).

California v. Greenwood, 486 U.S. 35 (1988).

Ciraolo v. California 476 U.S. 207 (1986).

Cruzan v. Director, Missouri Department of Health, 457 U.S. 261 (1990).

Eisenstadt v. Baird, 405 U.S. 438 (1972).

Gibson v. Florida Legislative Investigation Committee, 372 U.S. 539 (1963).

Goldman v. United States, 316 U.S. 129 (1942).

Griswold v. Connecticut, 318 U.S. 479 (1965).

Harlow v. Fitzgerald, 457 U.S. 800 (1982).

Katz v. United States, 389 U.S. 347 (1967).

Kyllo v. United States, 533 U.S. 27 (2001).

Laird v. Tatum, 408 U.S. 1 (1972).

Lawrence v. Texas, 539 U.S. 558 (2003)

Marsh v. Alabama, 326 U.S. 501 (1946).

McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).

Moore v. City of East Cleveland, 431 U.S. 494 (1977).

Myer v. Nebraska, 262 U.S. 390 (1923).

NAACP v. Alabama 357 U.S. 449 (1958).

Nixon v. Administrator of General Services, 433 U.S. 425 (1977).

Norwood v. Harrison, 413 U.S. 455 (1973).

Olmstead v, Unites States, 277 U.S. 438 (1928).

On Lee v.United States, 343 U.S. 747 (1952).

Paul v. Davis, 424 U.S. 693 (1976).

Public Utilities Commission v. Pollak 343 U.S. 451 (1952).

Roe v. Wade, 410 U.S. 113 (1973).

Schmerber v. California, 384 U.S. 757 (1966).

Silverman v. United States, 365 U.S. 505 (1960).

Smith v. Maryland, 442 U.S. 735 (1979).

Steagald v. United States, 451 U.S. 204 (1981).

Talley v. California, 362 U.S. 60 (1960).

Terry v. Ohio, 392 U.S. 1 (1868).

United States v. Miller, 425 U.S. 435 (1976).

United States v. White, 401 U.S. 745 (1971).

U.S. Dept. of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).

Washington v. Glucksburg, 521 U.S. 707 (1997).

Watchtower Bible & Tract Society of New York, Inc. v. Village of Stratton, 536 U.S. 150 (2002).

Whalen v. Roe, 429 U.S. 589 (1977).

U.S. Circuit Courts of Appeal

Alexander v. Peffer, 993 F.2d 1348 (8th Cir. 1993).

American Constitutional Law Foundation v. Meyer, 120 F.3d, 1092 (10th Cir. 1997).

Anderson v. Romero, 72 F.3d 518 (7th Cir. 1995).

Barry v. City of New York, 712 F.2d. 1554 (2nd Cir. 1983).

Borucki v. Ryan, 827 F.2d 836 (1st Cir. 1987).

Cutshall v. Sundquist, 193 F.3d 466 (6th Cir. 1999).

Denius v. Dunlap, 209 F.3d 944, 955 (7th Cir. 2000).

Douglas v. Dobbs, 419 F.3d 1097 (10th Cir. 2005).

Eagle v. Margan, 88 F.3d 620 (8th Cir. 1996).

Fadjo v. Coon, 633 F.2d 1172 (5th Cir. 1981).

Gruenke v. Seip, 225 F.3d 290 (3rd Cir. 2000).

Herring v. Keenan, 218 F.3d 1171 (10th Cir. 2000).

James v. City of Douglas, 941 F.2d 1539 (11th Cir. 1991).

J.P. v. DeSanti, 653 F.2d 1080 (6th Cir. 1981).

National Federation of Federal Employers v. Greenberg, 983 F.2d 286 (D.C. Cir. 1993).

Plante v. Gonzales, 575 F.2d. 1119 (5th Cir. 1978).

Russell v. Gregoire, 124 F.3d 1079 (9th Cir. 1997).

Schacter v. Whalen, 581 F.2d 35 (2d Cir. 1978).

Sterling v. Borough of Minersville, 232 F.3d. 190 (3rd Cir. 2000).

Tavoulareas v. Washington Post Co., 724 F.2d 1010 (D.C. Cir. 1984).

United States v. Westinghouse Electric Corporation, 638 F.2d 570 (3rd Cir. 1980).

U.S. District Courts

Roe v. Ingraham, 403 F.Supp. 931 (D.C.N.Y. Aug. 13, 1975).

Tatum v. Laird, 444 F.2d 947, 950 (C.A.D.C. Apr. 27, 1971).

Legislative Hearings

Jeffrey Rosen, Statement, Data Mining: Current Applications and Future Possibilities: Hearing Before the House Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census, Comm. on Gov't Reform, 108th Cong. (2003).

Securing Freedom and the Nation: Collection Intelligence Under the Law: Hearing Before the House Perm. Select Comm. on Intelligence, 108th Cong. (2003) *available at* http://intelligence.house.gov/PDF/martin040903.pdf .

Dr. Tony Tether, Director, DARPA, Written Statement Submitted to the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census of the House Committee on Government Reform (May 6, 2003), http://reform.house.gov/UploadedFiles/DARPA%20testimony.pdf.

Government Reports, Memoranda, Presentations, and Press Releases

John Ashcroft, Memorandum from John Ashcroft, U.S. Attorney General, to heads of department programs, *Guidelines for Disclosure of Grand Jury and Electronic and Oral Interception Information Identifying United States Persons* (Sept. 23, 2002), *available at* http://www.usdoj.gov/olp/section203.pdf.

Defense Advanced Research Projects Administration overview presentation to TAPAC, http://www.sainc.com/tapac/library/TerrorismInformationOverview.pdf

Final Report of the National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report (Authorized 1st Ed., 2004).

GAO, *Data Mining: Federal Efforts Cover a WideRange of Uses* , GAO-04-548 (2004).

GAO, *Data Mining, Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*, GAO-05-866 (2005).

GAO, *OMB Leadership Needed to Improve Agency Compliance*, GAO-03-304 (2003).

Memorandum from the Attorney General to Robert S. Mueller, Director of the FBI (Sept. 18, 2003), http://www.cdt.org/security/usapatriot/030918doj.shtml.

National Security Law Unit, Office of the General Council, FBI, Memorandum to National Security Division, FBI, on Guidance Regarding the Use of Choicepoint for Foreign Intelligence Collection or Foreign Counterintelligence Investigations (Sept 17, 2001), http://www.epic.org/privacy/publicrecords/cpfcimemo.pdf.

John M. Poindexter, speech, *Security with Privacy*, http://www.maxwell.syr.edu/campbell/library%20Papers/event%20papers/ISHS/Poindexter.pdf.

John M. Poindexter, speech, DARPATech 2002 Conference (Aug. 2, 2002), http://www.fas.org/irp/agency/dod/poindexter.html.

Sec'y of Def., Attorney Gen. & Dir. of Cent. Intelligence, Report to Congress Regarding the Terrorism Information Awareness Program: In Response to Consolidated Appropriations Resolutions, 2003, Pub. L. No. 108-7, Division M, §111(b) 27-35 (2003).

Staff of the Office of the Director of National Intelligence, The National Intelligence Strategy of the United States of America: Transformation though Integration and Innovation (October, 2005), http://www.dni.gov/NISOctober2005.pdf.

Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* (Mar. 2004), http://www.cdt.org/security/usapatriot/20040300tapac.pdf.

U. S. Dep't of Health, Education & Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Community on Automated Personal Data Systems* 9-10 (1973).

U. S. Dep't of Defense, *Report to Congress regarding the Terrorism Information Awareness Program*, May 20, 2003, http://www.darpa.mil/body/tia/tia_report_page.htm.

U. S. Dep't of Justice, Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, http://www.usdoj.gov/olp/generalcrimes2.pdf.

U. S. Dep't of Justice, Fact Sheet: Shifting from Prosecution to Prevention, Redesigning the Justice Department to Prevent Future Acts of Terrorism (2002), http://www.usdoj.gov:80/ag/speeches/2002/fbireorganizationfactsheet.htm.

Interest Groups

Center for Democracy and Technology, *Commercial Access to Information,* http://www.cdt.org/security/guidelines/final_commercial_matrix.shtml.

Center for Democracy and Technology, *Law Enforcement and Intelligence Access to Information,*http://www.cdt.org/security/guidelines/final_government_matrix.shtml.

Markle Foundation Task Force, Protecting America's Freedom in the Information Age (Oct. 2002), http://www.markletaskforce.org/.

Markle Foundation Task Force, Creating a Trusted Information Network for Homeland Security: Second Report of the Markle Foundation Task Force (Dec, 2003), http://www.markletaskforce.org/.

OpenTheGovernment.Org: Americans for Less Secrecy, More Democracy, report, Secrecy Report Card 2005: Quantitative Indicators of Secrecy in the Federal Government, http://www.openthegovernment.org/otg/SRC2005.pdf, last accessed 12/31/05.

Secondary Sources

Books

Brin, David, *The Transparent Society: Will Technology Force us to Choose Between Privacy and Freedom?* Addison-Wesley: Reading; 1998.

DeCew, Judith Wagner, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press: Ithaca and London, 1997.

Etzioni, Amitai, *The Limits of Privacy*. Basic Books: New York, 1999.

Garfinkle, Simson, *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly: Sebastopol, CA., 2001.

Glenn, Richard A., *The Right to Privacy: Rights and Liberties Under the Law*. ABC: Clio, 2003.

Larson, Erik, *The Naked Consumer: How our Private Lives Become Public Commodities*. Holt: New York, 1992.

Nock, Stephen L., *The Costs of Privacy, Surveillance and Reputation in America*. A. De. Gruyter: New York, 1993.

O' Harrow, Jr., Robert, *No Place to Hide*. Free Press: New York, 2005.

Rosen, Jeffrey, *The Unwanted Gaze: The Destruction of Privacy in America*. Random House: New York, 2000.

———, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*. Random House: New York, 2004.

Smith, Robert Ellis., *Ben Franklin's Website: Privacy and Curiosity from Plymouth Rock to the Internet*. Privacy Journal: Providence, RI., 2000.

Solove, Daniel J., *The Digital Person: Technology and Privacy in the Information Age*. New York University Press: New York, 2004.

Solove, Daniel J. and Marc Rotenberg,. *Information Privacy Law*. Aspen Publishers: New York, 2003.

Strum, Phillipa, *Privacy: The Debate in the United States Since 1945*, ed. Gerald W. Nash and Richard E. Etulain, Eds. (Harcourt Brace College Publishers: New York, 1998).

Sykes, Charles J., *The End of Privacy*. St. Martin's Press: New York,1999.

Westin, Alan F., *Privacy and Freedom.* Atheneum: New York, 1967.

Articles

Allen, Anita L.,"Privacy as Data Control: Conceptual ,Practical, and Moral Limits of the Paradigm," *Connecticut Law Review,* 32 (2000): 861-875.

Baker, C. Edwin, "Scope of the First Amendment Freedom of Speech," *UCLA Law Review*, 25 (1977-78): 964-1040.

Beermann, Jack M.,"Private Parties as Defendants in Civil Rights Litigation: Why do Plaintiffs Sue Private Parties Under Section 1983?," *Cardozo Law Review* 26 (2004): 9-34.

Burch, Thomas V., "Doublethink"ing Privacy Under the Multi-State Antiterrorism Information Exchange," *Seton Hall Legislative Journal* 29 (2004): 147-191.

Clarke, Roger A., "Information Technology and Dataveillance," *Communication of the ACM*, Vol.31, No. 5, (May 1988): 498-512.

Cohen, Julie E., "Examined Lives: Informational Privacy and the Subject as Object," *Stanford Law Review*. 52 (2000): 1373-1438.

———, "Privacy, Ideology, and Technology: A Response to Jeffrey Rosen," *Georgetown Law Journal* 89 (2001): 2029-2045.

———, "DRM and Privacy," *Berkeley Technology Law Journal* 18 (2003): 575-617.

Dempsey, James X., and Laura M. Flint, "Commercial Data and National Security," *George Washington Law Review* 72 (2004): 1459-1502.

Ervin, Jr., Sam J., "The First Amendment: A Living Thought in the Computer Age," in Surveillance, Dataveillance, and Personal Freedoms: Use and Abuse of Information Technology, eds. staff, *Columbia Human Rights Law Review* 23 (1972).

Froomkin, Michael, "The Death of Privacy?," *Stanford Law Review* 52 (2000): 1461-1543.

Fulda, Joseph S., "Data Mining and Privacy," *Albany Law Journal of Science and Technology* 11 (2000): 105-113.

Henderson, Stephen E., "Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search," *Mercer Law Review* 56 (2005): 507-563.

Hentoff, Nat, foreword*, Surveillance, Dataveillance, and Personal Freedoms: Use and Abuse of Information Technology*, Columbia Human Rights Law Review, eds. Staff, 23 (1972).

Hoofnagle, Chris Jay, "Big Brother's Little Helper: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement," *North Carolina Journal of International Law and Commercial Regulation* 29 (2004): 595-635.

Horn, Gayle, "Online Searches and Offline Challenges: The Chilling Effect, Anonymity and the New FBI Guidelines," 60 *New York University Annual Survey of American Law* 60 (2005): 735-778.

Karas, Stan, "Privacy, Identity, Databases," *American University Law Review* 52 (2002): 393-445.

Kerr, Orin S.,"The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," *Michigan Law Review* 102 (2004): 801-888.

Kramer, Irwin R., "The Birth of Privacy Law: A Century since Warren and Brandeis," *Catholic University Law Review* 30 (1990): 703.

.

Kreimer, Seth, "Watching the Watchers: Surveillance, Transparency, and Political Freedom in the War of Terror," *University Pennsylvania Journal of ConstitutionalL aw* 7 (2004):133-181.

Ku, Raymond Shih Ray, "The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance," *Minnesota Law Review* 86 (2002): 1325-1378.

Lardiere,Eric, "The Justiciability and Constitutionality of Political Intelligence Gathering," *University of California at Los Angeles Law Review* 30 (1983): 976-1051 .

McClurg, Andrew J., "A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling," *Northwestern University Law Review* 98 (2003): 63-143.

Miller, Arthur R., "*Computers, Data Banks and Individual Privacy: An Overview,"* in Surveillance, Dataveillance, and Personal Freedoms: Use and Abuse of Information Technology, eds. Staff, *Columbia Human Rights Law Review* 11 (1972).

Murphy, Richard S., "Property Rights in Personal Information: An Economic Defense of Privacy," *Georgetown Law Journal* 84 (1996): 2381-2417.

Podesta, John D., and Raj Goyle, "Lost in Cyberspace? Finding American Liberties in a Dangerous Digital World," *Yale Law and Policy Review* 23 (2005): 509-527.

Post, David G., "What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace," *Stanford Law Review* 52 (2000): 1439-1459.

Prossor, William J. "Privacy," *California Law Review*. 48 (1960): 383.

Richards, Neil M., "Reconciling Data Privacy and the First Amendment," *University of California at Los Angeles Law Review* 52 (2005): 1149-1222.

Rosenzweig, Paul S., "Proposals for Implementing the Terrorism Information Awareness System," *Georgetown Journal of Law and Public Policy* 2 (2004): 169-200.

———, "Civil Liberty and the Response to Terrorism," *Duquesne Law Review* 42 (2004): 663-723.

Rotenberg, Marc, "Privacy and Secrecy After September 11—Foreword: Modern Studies in Privacy Law," *Minnesota Law Review* 86 (2002): 1115-1135.

Schwartz, Paul M., "Privacy and Democracy in Cyberspace," *Vanderbilt Law Review* 52 (1999): 1607-1702.

———, "Free Speech v. Information Privacy: Eugene Volokh's First Amendment Jurisprudence," *Stanford Law Review* 52 (2000): 1559-1572.

———, "Property, Privacy, and Personal Data," *Harvard Law Review* 117 (2004): 2055-2128.

Solove, Daniel J., "Privacy and Power: Computer Databases and Metaphors for Information Privacy," *Stanford Law Review* 53 (2001): 1393-1462.

———, "Access and Aggregation: Public Records, Privacy and the Constitution," *Minnesota Law Review* 86 (2002): 1137-1218.

———, "Conceptualizing Privacy," *California Law Review* 90 (2002): 1087-1155.

———, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," *Southern California Law Review* 75 (2002): 1083-1167.

———, "Surveillance Law: Reshaping the Framework," *George Washington Law Review* 72 (2004): 1264-1305.

———, "Data Privacy and the Vanishing Fourth Amendment," *Champion* 49 (May 2005): 20.

Soma, John T., et. al., "Balance of Privacy vs. Security: A Historical Perspective of the USA Patriot Act," *Rutgers Computer and Technology Law Journal* 31 (2005): 285-345.

Steinberg, David E., "Making Sense of Sense Enhanced Searches," *Minnesota Law Review* 74 (1990): 563-629.

Strahilevitz, Lior Jacob, "A Social Networks Theory of Privacy," *University of Chicago Law Review* 72 (2005): 919-988.

Taipale, K. A., "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data," *Columbia Science and Technology Law Review* 5 (2004): 2, http://www.stlr.org/cite.cgi?volume=5&article=2

———, "Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of Old King Ludd," *Yale Symposium on Law and Technology* 7 (2004/2005): 123-216.

Tien, Lee, "Privacy, Technology and Data Mining," *Ohio Northern University Law Review* 30 (2004): 389-415.

Volokh, Eugene, "Freedom of Speech and Information Privacy: The troubling implications of a Right to Stop People from Speaking about You," *Stanford Law Review* 52 (2000): 1049-1124.

Warren, Samuel,and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4 (1890): 193.

Weiss, Charles, "The Coming of Knowledge Discovery: A Final Blow to Privacy Protection?" *University of Illinois Journal of Law, Technology, and Policy* 2004 (2004): 253- 281 .

Zarsky, Tal Z., "Mine Your Own Business!: Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion," *Yale Symposium on Law and Technology* 5 (2002/2003): 1.

———, "Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining," *Maine Law Review* 56 (2004):13-59.

———, "Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society," *University of Miami Law Review* 58 (2004): 991-1044.

Other Media

David Jensen, slideshow, *Data Mining in Networks* (December 11, 2002), http://kdl.cs.umass.edu/people/jensen/papers/nrcdbsse02/slide10.html.