NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MINDING THE GAP: THE GROWING DIVIDE BETWEEN PRIVACY AND SURVEILLANCE TECHNOLOGY

by

Debra Kirby

June 2013

Thesis Advisor: Christopher Bellavita
Second Reader: Donald Zoufal

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE MINDING THE GAP: THE GROWING DIVIDE BETWEEN PRIVACY AND SURVEILLANCE TECHNOLOGY		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Debra Kirby			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Pervasive mass surveillance in a given in U.S. society. However, whether U.S. citizens sacrifice privacy as a result remains under debate. Does privacy fade away in light of the connected world in which we all live? The recent U.S. Supreme Court decision in *U.S. v. Jones* did not address whether pervasive mass surveillance by the government constituted a search under the Fourth Amendment, and, thereby, triggering constitutional review. The lack of legal guidance presents challenges for law enforcement investigations, as it can takes years for a court to decide a privacy case and surveillance technology evolves at a far more rapid pace. Given the refusal, or inability, of the courts to answer what constitutional privacy protections are afforded U.S. citizens in light of the growing use of sensor technology to conduct mass surveillance, inclusive of GPS, RFID, and LPR, comprehensive legislative privacy options must be explored. To date, privacy has been left to the individual states, which results in privacy protections based upon geography. Federal privacy legislation is limited, focusing on certain technologies, such as eavesdropping under Title III, or certain privacy issues, such medical record data under HIPAA. Further, very few laws govern the use and dissemination of the PII data that derives not only from governmental surveillance, but also from commercial data collection. A federal data protection act would define the privacy interests protected, rather than using the law to limit the government's specific use of a surveillance technology, which would ensure that the rules of engagement for the government surveillance were clear and held the government accountable to its citizens.

14. SUBJECT TERMS Privacy, Technology, Fourth Amendment, Governmental Surveillance, Sensor Technology, Mass Surveillance, Law Enforcement, Law Enforcement Investigations, Legislative Privacy Protections, Judicial Review, Data Aggregation, Data Privacy, PII, GPS, LPR, Data Collection, Data Analysis, Data Protection Statute			**15. NUMBER OF PAGES** 185
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

MINDING THE GAP: THE GROWING DIVIDE BETWEEN PRIVACY AND SURVEILLANCE TECHNOLOGY

Debra Kirby
Chief, Bureau of Organizational Development Chicago Police Department, Chicago, IL
B.S., University of Illinois, 1984
J.D., John Marshall Law School, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN HOMELAND SECURITY
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
June 2013

Author: Debra Kirby

Approved by: Christopher Bellavita
Thesis Advisor

Donald Zoufal
Second Reader

Harold A. Trinkunas, PhD
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Pervasive mass surveillance in a given in U.S. society. However, whether U.S. citizens sacrifice privacy as a result remains under debate. Does privacy fade away in light of the connected world in which we all live? The recent U.S. Supreme Court decision in *U.S. v. Jones* did not address whether pervasive mass surveillance by the government constituted a search under the Fourth Amendment, and, thereby, triggering constitutional review. The lack of legal guidance presents challenges for law enforcement investigations, as it can takes years for a court to decide a privacy case and surveillance technology evolves at a far more rapid pace. Given the refusal, or inability, of the courts to answer what constitutional privacy protections are afforded U.S. citizens in light of the growing use of sensor technology to conduct mass surveillance, inclusive of GPS, RFID, and LPR, comprehensive legislative privacy options must be explored. To date, privacy has been left to the individual States, which results in privacy protections based upon geography. Federal privacy legislation is limited, focusing on certain technologies, such as eavesdropping under Title III, or certain privacy issues, such medical record data under HIPAA. Further, very few laws govern the use and dissemination of the PII data that derives not only from governmental surveillance, but also from commercial data collection. A federal data protection act would define the privacy interests protected, rather than using the law to limit the government's specific use of a surveillance technology, which would ensure that the rules of engagement for government surveillance were clear and held the government accountable to its citizens.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
AFIS	Automated Fingerprint Identification System
AIDC	Automatic Identification and Data Capture
ANPR	Automatic Number Plate Recognition
CBP	Custom and Border Patrol
CCTV	Closed Circuit Television Surveillance
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DHS TRIP	DHS Traveler Redress Inquiry Program
DNA	Deoxyribonucleic Acid
DNI	Director of National Intelligence
DoD	Department of Defense
DPA	Protection Act of 1998
ECHR	European Convention of Human Rights
ECPA	The Electronic Communications Privacy Act
EDL	Enhanced Driver's Licenses
EDR	Event Data Recorder
EU	European Union
FBI	Federal Bureau of Investigation
FOIA	Freedom of Information Act
FRT	Facial Recognition Technology
GLBA	Gramm–Leach–Bliley Act
GPS	Global Positioning Satellite
HIPAA	Health Insurance Portability and Accountability Act
HLS	Homeland Security
IACP	International Association of Chiefs of Police
IP	Internet Protocol
LPR	License Plate Recognition
MORIS	Mobile Offender Recognition and Information System
MRZ	Machine Readable Zone
NIJ	National Institute of Justice
NSTC	National Science and Technology Council

PII	Personally Identifiable Information
RFID	Radio Frequency Identification
SBInet	Secure Border Initiative
SCA	Stored Communications Act
TSA	Transportation Security Administration
U.K.	United Kingdom
U.S.	United States
UAS	Unmanned Aircraft Systems
WHTI	Western Hemisphere Initiative

EXECUTIVE SUMMARY

Pervasive mass surveillance is a given in United States (U.S.) society. Whether U.S. citizens sacrifice privacy rights as a result remains under debate. Technology continues to push the boundaries of individual privacy. The government's use of mass pervasive surveillance technology brings forth significant challenges for the legal framework that addresses the privacy of U.S. citizens. In today's increasingly networked society, an abundance of personally identifying information (PII),[1] is generated and increasingly subject to sophisticated analytic techniques, which in turn, drives further technology innovations (Consumer Data Privacy in a Networked World, 2012, p. 5). Yet, the legal response to the government's use of surveillance technology innovations is not only slow, but it also relies upon incremental judicial review tethered to older technology. This tension between technology innovation and slow legal response continues unabated.

The viability of legal protections for individual privacy is in question given that the U.S. Supreme Court continues to voice concerns about technology's encroaching impact upon privacy yet continues to fail to provide proper guidance for the government. The U.S. Supreme Court's recent decision in *United States v. Jones* demonstrates that it seeks to narrow privacy issues before it rather than broadly address the privacy impact of surveillance technology used by government (*United States v. Jones*). Additionally, the legislative response is not much better in that a patchwork of federal and local law addresses privacy in a piecemeal fashion, thereby failing to address comprehensively what is individual privacy in a digital world. This lack of sufficient legal guidance is troubling for law enforcement as well, in that technology investment, and its use for criminal investigations, is subject to a wait and see process as the various privacy claims traverse through the U.S. legal system. The delay in legal decision and guidance results in financial costs, given technology investments by the government, and social costs, given

[1]For purposes of this thesis, PII is defined as any information about an individual that can be used to distinguish or trace an individual's identity, including, but not limited to, name, social security number, date and place of birth, mother's maiden name, or biometric records, and (2) any other information linked or linkable to an individual, such as medical, educational, financial, and employment information (Grance et al., 2010, p. ES-1).

that surveillance actions continue while under legal review. Such processes fail to serve either the government's public safety needs or individual privacy protections. As a consequence, whether privacy degrades to a pleasant antiquated concept, or whether it emerges as something expressly defined and protected within the modern linked world, remains to be seen.

Privacy determinations under the Fourth Amendment take years and the individual legal skirmish lines drawn with each new surveillance technology and its use create uncertainty both for the government and for individual privacy. Constitutional law and, more specifically, Fourth Amendment doctrine has been the traditional vehicle for holding the government accountable for intrusions into the private lives of its citizens. A labyrinth process, constitutional review can take years from an initial claim to final legal outcome. Additionally, judicial review is an incremental process, predicated upon specific fact patterns and precedential decision, which may or may not translate to a general rule or guidance on the government's use of surveillance technology. Finally, the judicial outcome may ultimately fail to address the key privacy issue, as seen in the Supreme Court's decision in *Jones*, where the Court declined to address the privacy impact resulting from the government's use of global positioning satellite technology, (GPS), to conduct surveillance.

Technology presents a different context and challenge for Fourth Amendment review. The seminal Fourth Amendment decision of the U.S. Supreme Court in *Katz v. United States* is predicated upon the government's use of eavesdropping devices on landline telephones, hardly in line with current surveillance technology (*Katz v. United States*). Further, judicial review focuses on the specific technology before it, while the precedent-based legal system seeks to use prior decisions to support current legal outcome. In applying the *Katz* standard of reasonableness to increasingly invasive and advancing forms of technology, the courts have generated a line of legal decisions that are sometimes seen as inconsistent. In part, advances in technology are not fully evaluated for their unique privacy impact, but rather are linked to past decisions, as based upon relevance as identified by the court. Further, the courts may or may not be informed fully as to the technology and its use within society, yet are deciding its privacy impact.

For example, GPS does not operate under the same technology as a beeper, yet decisions in *United States v. Knotts* and *United States v. Karo,* which derive from older beeper tracking technology, are used to review privacy claims arising out of the government's use of GPS for surveillance, as discussed within *United States v. Garcia*. (*United States v. Knotts*; *United States v. Karo*; *United States v. Garcia*). While such actions result in legal efficiencies, they may not properly address the privacy impact that technology innovations bring forth.

General privacy protections have been left to the jurisdiction of the individual states, which results in protections based upon geography rather than standard privacy principles. Not only do differing state standards negatively impact criminal investigations in an increasingly mobile world, the practical result is that the most restrictive state law controls a criminal surveillance investigation anticipated to cross state borders. Existing federal privacy legislation is limited in jurisdiction and scope, focusing on certain technologies, such as law enforcement eavesdropping under Title III of the Omnibus Crime Control and Safe Streets Act of 1968[2] or certain privacy issues, such as medical record data under Health Insurance Portability and Accountability Act of 1996, (HIPAA).[3] Recent legislative attempts have been made to exercise federal jurisdiction over certain surveillance technology, as seen with recent Congressional attempts to pass the Geolocation Privacy and Surveillance Act.[4] However, focus on a specific technology serves little privacy value long term in that technology evolves quicker than subsequent legislative address, as seen with the limitations of Title III and its limited scope.

The aggregation and subsequent secondary use of data generated by the government's use of sensor technology for surveillance is a new privacy frontier and creates unique privacy problems. Very few laws govern the use and dissemination of the PII data derived from mass surveillance. Given its prevalence and ability to aggregate and individuate data across distinct technology systems, modern mass surveillance technology increasingly blurs the Fourth Amendment's focus on what is publicly

[2] Pub. L. No 90-351, § 802, 82 Stat. 212. 18 U.S.C. §§ 2510, et al. (1968, 2010).

[3] Pub. L. No. 104-191, §§ Pub. L. No. 104-191, 110 Stat. 1936 (1996)).

[4] 112th Congress (2011–2012) S.1212 and H.R. 2168.

disclosed and what is not (The Constitution Project, 2011, p. 2). Additionally, the collection and use of PII is not limited to the government, as numerous consumer outlets and other private entities generate increasing amounts of PII. The Fourth Amendment does not apply to private entities and minimal legal restrictions exist to guide and restrict the growing data information industry.

Given the refusal, or inability, of the courts to answer what constitutional privacy protections are afforded U.S. citizens, and in light of the growing use of sensor technology to conduct mass surveillance, inclusive of GPS, radio frequency identification, (RFID), and automated license plate readers, (LPR), comprehensive legislative options that address privacy must be explored. A variety of options exist to address the growing challenge of protecting privacy given the expansive of pervasive mass surveillance, but none are all encompassing. The options include 1) self-governance over the use of sensor technology, 2) use of the judicial process to continue to define the limits of the government's use of surveillance technology under existing Fourth Amendment doctrine, 3) state control and definition of the privacy protections afforded their citizens, or, 4) enacting comprehensive federal legislation to address the government's use of sensor technology and the derivative PII data that results. Of these four options, the first has negligible accountability for those establishing self-governed standards. The second and third options represent the status quo, and provide minimal direction for law enforcement, and do not afford additional safeguards for civil liberties. The fourth option, while providing long-term protection for privacy, requires political will to address an increasingly complex legal and social problem.

A federal data protection act would serve to define the privacy interests protected, rather than using the law to limit the government's specific use of a surveillance technology. Such legislation would ensure that the rules of engagement for government surveillance were clear and would hold the government accountable to its citizens. Unlike a Fourth Amendment review, which must first identify whether a protected privacy interest exists, a data protection act defines the privacy interests protected and the applicable legal standards. Therefore, the law becomes a means to protect privacy by identifying when the privacy interest is substantial enough to demand state action rather

than state neutrality (Taylor, 2011, p. 457). The judicial review then centers on the privacy interest and not in carving out specifications based on the government's use of a technology.

As technology changes, expectations of privacy may shift, but the underlying civil liberty protections for privacy should remain. A data protection act would not only define the privacy interests subject to protection but would establish clear guidance for lawful government action in regards to privacy standards regardless of the technology involved. Congress is in the unique position of being able to protect individual privacy, rather than merely limiting how the government uses a specific technology to conduct surveillance of its citizens. Exercise of federal jurisdiction over data privacy would ensure consistent, minimal standards for privacy protection with clear rules of engagement for all, including private entities. Given that the byproduct of mass surveillance technology, PII, and its use, is not comprehensively addressed in U.S. law, a federal data privacy protection act would ensure privacy protections for U.S. citizens in an increasingly globally networked society.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Chris and Don, thanks for helping me cross the line.

To the staff and my classmates at CHDS, thanks for allowing me to learn from all of you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Privacy is a concept that has been part of the popular legal discussion within the United States (U.S.) since Justice Brandeis' raised his concerns over the privacy invasion created by portable photography (Brandeis & Warren, 1890, p. 194). In a world in which the movement of individuals in public is tracked, often surreptitiously, the question is whether privacy is nothing but a radionuclide, left to decay amongst a world of bytes and monitors? In today's increasingly networked society, an abundance of personally identifying information, (PII),[5] is generated through increasingly sophisticated analytic techniques, which, in turn, drive more innovation (Consumer Data Privacy in a Networked World, 2012, p. 5). As a consequence, does privacy degrade to a pleasant antiquated concept, or does it emerge as something different, something specifically defined and protected, within the modern, linked world?

The concept of privacy has remained tenable within the legal system and in the culture of the United States, weathering the advent of various technologies from portable photography to deoxyribonucleic acid, (DNA). In 2012, the U.S. Supreme Court had the opportunity to weigh in and legally define the proper role and structure for government's use of sensor technology to conduct surveillance, thereby defining the privacy rights of citizens subject to governmental surveillance in *United States v. Jones*. The issue before the Court was centered on the government's use of geolocational positioning satellite technology, (GPS), to track an individual under criminal investigation without a warrant for a period of 28 days through multiple jurisdictions (*United States v. Jones*). Rather than the address the broader civil liberties and privacy concerns raised before the Court, it chose to decide the case on the narrower issue of physical trespass—tying the privacy issue and decision to how the government attached the GPS device, rather than how it used the device and information (*United States v. Jones*, pp. 949–951). In ignoring the

[5] For purposes of this thesis, PII is defined as any information about an individual that can be used to distinguish or trace an individual's identity, including, but not limited to name, social security number, date and place of birth, mother's maiden name, or biometric records, and (2) any other information linked or linkable to an individual, such as medical, educational, financial, and employment information (Grance, McCallister, & Scarfone, 2010, p. ES-1).

widespread use of GPS by law enforcement and the privacy concerns of those subject to such surveillance, the *Jones* Court expressly noted that the government's use of surveillance technology creates vexing privacy problems (*United States v. Jones*, p. 954). However, the Court found no need to address the privacy concerns raised before it, and identified that analysis of the vexing privacy issues may be needed in the future, but not presently (*United States v. Jones*, p. 954). As a result, the burgeoning privacy issues associated with law enforcement's use of GPS and other sensor technology in criminal investigations will continue to be resolved through an ad-hoc legal framework consisting of state and federal case and statutory law, public policy, and ongoing constitutional review through the courts. The outcome of such a system results in a lack of clear and consistent direction to those engaged in the investigation of criminal conduct, inclusive of terrorism. Such a system not only fails to guide proper governmental action, it also fails to protect civil liberties.

A. PROBLEM STATEMENT

Technology is inanimate, but how technology is used can create significant societal impact. The growing use of surveillance technology and its privacy impact is of increasing concern, not only over the act of observation itself, but also over the subsequent use and retention of the data collected. While government surveillance is not new, the older technologies used by the government to conduct surveillance were not as intrusive as those in use today. Today's surveillance technology can be used to track the public movement of citizens easily through time and space, using technologies, such as GPS or license plate recognition systems, (LPR). The U.S. legal system and its practice of *stare decisis*[6] (Cornell University Law School, 2010) places significant reliance upon decisions derived from the government's use of older technologies, including automated fingerprint information systems, (AFIS), and closed circuit video, (CCTV). However, these decisions provide minimal privacy guidance for the rapidly expanding capacity of the modern technology used by the government to monitor the public movement of its

[6] *Stare decisis* is a legal doctrine that obligates courts to follow precedent. Courts will follow and cite to *stare decisis* when an issue has been previously brought to the court, or a higher court, and a ruling already issued. Generally, courts will adhere to their previous rulings, although not universally true. (Legal Information Institute, 2010).

citizens. The meteoric rise of new technology both generates new privacy concerns (through the creation of new forms of sensitive data) and renders certain privacy concerns related to older technology (that is no longer used) less relevant (Serwin, 2009, p. 876). Today's sensor technology, inclusive of computerized record systems and advanced data aggregation, creates more individuated data (Schwartz & Solove, 2011, p. 1821). The aggregation and subsequent secondary use of data generated by the government's use of sensor technology for surveillance creates unique privacy problems.

As rapidly as technology is being developed and refined, it is being deployed and used within the homeland security (HLS) field. However, as demonstrated in the U.S. Supreme Court decision, *United States v. Jones*, the courts remain unwilling to, or incapable of, addressing the broader issue of privacy protections when reviewing the government's use of technology to conduct surveillance. The U.S. Supreme Court continues to kick the can down the road, by recognizing that technology creates novel issues that must be addressed, yet refuses to do so (*United States v. Jones*, p. 954). As a result, a burgeoning gap grows between legal policy and operational practice for the government's use of sensor surveillance, which has significant HLS impact given the intertwined issues of technology, surveillance, and privacy.

1. Government's Use of Technology

The use of technology within the field of HLS has become ubiquitous. The Department of Homeland Security (DHS) is committed to investing in sensor technology (Border Security, 2010). DHS has installed closed circuit television monitoring (CCTV) and other sensor technology at the southern borders under the Secure Border Initiative (SBInet)[7] (Lipowicz, 2011). The Customs and Border Patrol (CBP) and the Transportation Security Administration (TSA) rely upon a variety of technologies, inclusive of CCTV, biometric identification technologies, scanners, and other developing technologies to help identify individuals and contraband (Transportation Security Administration, 2008). The TSA's advanced imaging technology, or body scanners, in

[7] SBInet was DHS driven technology effort focused on the areas along the Southwest Border of the United States, with a goal to use technology to leverage border resources in an effort to secure the borders (U.S. Customs and Border Patrol, SBInet Block 1).

which air travelers are scanned with full skeletal outline, are another example of the TSA's growing technology investment to support of HLS functions. Even amidst an aggressive roll out of current technology, the TSA continues to look for new technology to address its overall mission, given a belief that technology reduces emerging HLS threats (Transportation Security Administration, 2008).

Local governments also use sensor technology for a variety of purposes. The use of CCTV in support of public safety is prevalent in cities, such as New York and Chicago (Cameron, Kolodinski, May, & Williams, 2008, pp. 5–6). LPRs are used within a variety of jurisdictions (IACP, 2009, pp. 5–6). GPS is used by both local and federal law enforcement for criminal investigations and other public safety purposes, e.g., monitoring parolees (Koppel, 2010, pp. 1065–1066; Smith, 2011, pp. 1–3). GPS is also used for a variety of administrative purposes ranging from mobile asset tracking (Thomas, 2007) to identifying pothole locations (Breier, 2011). Another form of sensor technology, radio frequency identification systems (RFID), which allow for identification at a distance, is being used for a variety of purposes, including inventory and payment of toll fares (Brito, 2004, pp. 6–7). New York state currently embeds RFID into their "enhanced driver's licenses," (EDL), which allow U.S. citizens entry from Canada, Mexico and the Caribbean for other than air travel (New York State Department of Motor Vehicles, n.d.). Public safety agencies also continue to explore and test newer sensor technologies, such as facial recognition technology, (FRT), and iris scanning, in support of their public safety and homeland security missions (Steele, 2011). Given the rapid development and use of sensor technology, the complexity and capacity to individuate sensor data will continue to grow, as will the associated privacy concerns when the government uses technology to conduct mass surveillance.

2. Legal Response

The government's use of surveillance technology, which facilitates mass monitoring and limits individual control over access to and use of PII information, is a privacy trigger. Privacy can be defined as a function of the ability to control access to or information about an individual (A. Moore, 2008, p. 414). The government's monitoring

of individual movement in public spaces, through the observation, recording, and reporting of such data, limits an individual's control over anonymity in public space. The courts have recognized that the advance of technology affects the degree of privacy secured to citizens by the Fourth Amendment (*Kyllo v. United States*, pp. 33–34). What the courts and Congress have failed to define is to what degree that impact comports with constitutional protections. In a society wherein the boundaries of what is public and what is private is being revolutionized as a result of technological development, the failure to define privacy protections legally is a significant gap.

Modern technology allows government to monitor the movement of mass numbers of its citizens unobtrusively with relative ease. Existing Fourth Amendment law limits the right of government intrusion upon its citizens through analysis of that which is and is not "knowingly made public" (*Katz v. United States*, p. 351). However, sensor technology, such as GPS, enables the public movement of individuals to be tracked in detail across time, distance and location (Hutchins, 2007, p. 414). The level of detail available through government surveillance of the public movement of its citizens, both as a matter of initial collection, and in particular, given the ability to aggregate and individuate data across distinct technology systems, increasingly blurs the Fourth Amendment's focus on what is publicly disclosed and what is not (The Constitution Project, 2011, p. 2). In part, this situation results because privacy issues enter the legal system piecemeal, as individual cases with specific facts, which influence the overall body of law. As a result, the degree to which technology impacts individual privacy has yet to be fully determined, both as a matter of precedential law and as a matter of governmental power. See *United States v. Jones* (pp. 953–954), with Justice Sotomayor concurring (pp. 956–957), and with Justice Alito concurring (pp. 962–963). The privacy impact of technology and the limitations on the government's use of technology to monitor the public movement of its citizens remains.

3. Fourth Amendment

The Fourth Amendment has traditionally been used to define permissible government action in relation to the privacy of its citizens. For Fourth Amendment

protections to apply, first, it must be determined whether the actions by the government constitute a search subject to constitutional protections, and then, whether the privacy expectations of the individual are reasonable (*Katz v. United States*). However, no shared, common definition exists for what constitutes a search, nor have the courts defined what constitutes a reasonable expectation of privacy in this age of mass surveillance (*United States v. Jones*). More disconcerting, is that the courts continue to provide limited and inconsistent direction for permissible government action in the protection of individual privacy (Hutchins, 2010, pp. 1186–1187). As a result, law enforcement is left to attempt to guess what constitutes a reasonable search when using modern technology. Constitutional analysis of the government's use of sensor technology to conduct mass surveillance remains dynamic; thereby, leaving a gap in the Fourth Amendment framework that determines the appropriate restraints on governmental surveillance.

4. State Privacy Protections

Constitutional law is not the sole legal vehicle to protect individual privacy. The determination and protection of any generalized right of privacy falls to the states (*Katz v. United States*, pp. 350–351). Given the reticence of the U.S. Supreme Court to provide guidance on the applicability of the Fourth Amendment to the government's use of modern surveillance technology, the states have responded, in varying measures, with local statutory protections. Some states, including California, allow only law enforcement the right to track a person electronically, with criminal penalties for those in violation of the law. See, e.g., California Penal Code section 637.7, Stats. 1998 c. 449 (S.B. 1667) § 2. Other states, including Pennsylvania, South Carolina, Minnesota, and Florida, use legislation to address how GPS may be used by law enforcement, with some mandating law enforcement officers obtain a warrant prior to using GPS to conduct surveillance. See, e.g., 18 Pennsylvania Constitutional Statute § 5761, South Carolina Code Annotated § 17-30-140, Minnesota Statute § 626A.37, §626A.35, and Florida Statute § 934.06, 934.42. Additionally, some states have moved to provide broader privacy protections to their citizens under state constitutions than currently available under the U.S.

Constitution (Gershman, 2010, p. 929). State statutory law is being used to address the privacy gaps generated by the use of modern surveillance technology that federal and constitutional law has not addressed.

The challenge with state-based privacy protections is that the individual laws and social mores are not homogenous and may vary from state to state. Competing and distinct state laws provide different privacy standards, which may be triggered by virtue of an individual crossing a state line. In a mobile society, such as the United States, locally determined privacy protections become a matter of determining geography, rather than base civil liberty protections or public policy. In turn, disparate laws negatively affect law enforcement's use of surveillance technology for criminal investigations (*United States v. Jones*, p. 931). Absent consistent legal standards, law enforcement is left to guess which law applies and when, or spend unnecessary resources trying to compensate for the rules of each anticipated jurisdiction of travel during a criminal investigation. The privacy impact of sensor technology will continue to be of concern as technology development outpaces the legal structure that defines what legal protections are afforded citizens under governmental surveillance.

5. Mass Monitoring—The Future is Now

Modern sensor technology allows the government to mass monitor the public movement of its citizens unobtrusively and consistently. CCTV, one of the first mass surveillance technologies, generated significant concern over the government's observation of the public movement of its citizens (Ozer & Schlosberg, 2007, pp. 1–2). However, unlike early CCTV, which was generally localized and had limited retention capacity, today's sensor surveillance technology allows for shared environments, multiple end-users, and significantly expanded use of the images obtained (Dwyer, La Vigne, Lowry, & Markman, 2011, pp. ix–x). GPS, LPR, and RFID all monitor the public movement of individuals through time, space, and distance, and each of these technologies can be combined with other technologies to create a public surveillance of significant scope and capacity (Ozer & Schlosberg, 2007, p. 1). As such, sensor technology raises issues not only over the government's initial intrusion and over the

monitoring of citizens in public space, but also in regards to the aggregation of PII data through leveraged use of other technologies; thereby, potentially creating a mosaic of information regarding the individual, with more information beyond the single observation.

Data mining and aggregation is of growing concern given the ability to augment the data developed by one surveillance system with that of another (*United States v. Jones*; *People v. Weaver*; Kerr, 2011; Posen, 2005). However, concerns over what may result from surveillance technology cannot ignore what already exists. Current technology in use allows for significant linkage and augmentation of a singly byte of data. The ability to individuate PII data, (e.g., to link the tollbooth collections data to the license plate of a registered owner to location of an individual for which a warrant exists), creates the potential for a larger, more comprehensive scope of surveillance of public movement by government (Ozer & Schlosberg, 2007, pp. 3–4). Such aggregation furthers public safety efforts in light of the mobility of the criminal population. Therefore, given the growing reliance upon sensor technology by the HLS field, the gap in consistent legal guidance and the variance in state statutes have significant consequence for civil liberties and public safety.

B. RESEARCH QUESTION

Is a federal privacy statute necessary to address the dual concerns of public safety and privacy given the government's increasing use of sensor technology that monitors the movement of individuals within public spaces?

C. PRACTICAL SIGNIFICANCE OF THE RESEARCH

Surveillance technologies continue to evolve, and will serve only to further heighten privacy concerns. This thesis conducts an in-depth analysis of the existing law and policy regarding the government's use of sensor technologies, including GPS, to monitor the movement of people across public spaces. Public safety and civil liberties are not mutually exclusive. However, as technology becomes more advanced, and the government's mass monitoring of its citizen's movement in public spaces becomes more prevalent, defining the appropriate boundaries for privacy better ensures the protection of

civil liberties. Despite its prevalent use within law enforcement, even the use of GPS remains a Fourth Amendment frontier without defined legal boundaries, despite the opportunity for the U.S. Supreme Court to establish legal guidelines (*United States v. Jones*; *United States v. Cuervas-Perez*). Identifying general privacy goals and legal protections for individual privacy will stop the circular legal chase brought forth by the existing practice of identifying the privacy impact of how the government uses a specific technology. A legal framework that recognizes privacy rights, rather than reviews how government uses technology, will provide the appropriate legal guidance for the government's use of surveillance technology.

This thesis contributes to the emerging body of literature intent on analyzing the current and long-term issues associated with privacy and technology, and governmental surveillance of its citizen's public movements. By focusing on legal analysis, this thesis provides guidance for HLS professionals when making policy decisions regarding surveillance technology that will benefit not only the initial investigative objective and support prosecution and criminal deterrence, but will also comport with the traditional legal principles that have protected the civil liberties of U.S. citizens.

While the gap between government's use of surveillance technology and legal governance has implication for HLS policy, it has significant practical implications as well. In a time of unprecedented fiscal challenge, the government is looking to use technology as a means to not only reduce personnel costs, but to also leverage existing resources (Office of Community Oriented Policing Services, 2011, pp. 26–27). While technology supports efficiency in government, its implementation also brings forth significant cost (Zoufal, 2008, p. 124). For example, the costs of the CCTV systems within the various cities that have implemented such systems are well into the millions, with some cities, such as Chicago and New York, exceeding costs of tens of millions (Cameron et al., 2008, p. 6). Given that the law often lags behind technology development and use, contrary legal decisions over the government's use of sensor technology may result in a significant drain on public financial resources, particularly if the use is severely limited through judicial decision. Further, criminal investigations, prosecution and judicial outcome generate fiscal and social costs when the wrong

decision is made regarding the legality of the use of surveillance technology. The respondent Jones came under criminal investigation in 2003, was first before the court in 2006, and after several trials, the matter was finally resolved by the Supreme Court almost six years later (*United States v. Maynard*; *United States v. Jones*). Specific guidance on constitutional privacy requirements is optimally provided ahead of the government's technology investments, rather than subsequent to purchase and implementation, as is current legal practice.

Finally, while this thesis addresses significant privacy issues, many privacy issues regarding evolving technology remain unaddressed. George Orwell saw government as big brother—all watching (Orwell, 1949). However, complex technology systems exist, and growing enthusiasm is increasing for linking and sharing data amongst shared enterprise systems within the private domain, either independently for commercial purposes or in partnership with government (Digital Government, n.d.). Also significant private commercial growth is arising from the mega-data developed as a form of surveillance technology now in use.[8] The subsequent end use and retention of the data amassed from the multitude of surveillance technologies, both governmental and private, is a growing privacy concern. Constitutional limitations generally do not apply to private entities, and other legal restriction is minimal for said entities. Further, whether PII remains a valid touchstone for privacy boundaries and whether it remains subject to definition in light of the growing capacity for data aggregation, including the individuation of data previously non-identifying, raises new concerns for privacy protections (Schwartz & Solove, 2011). A federal data protection statute, applicable to both government and private entities, as proposed within this thesis, establishes basic privacy protections, and is necessary, given the growing use of surveillance technology and the PII data that it derives. Not only is this thesis topic an area ripe for legal intercession, it requires further research and review as technology takes on a more dominant role in U.S. society; thereby, further transforming the concept of privacy.

[8] For example, All State Insurance has recently offered discount opportunities under its "Drive Wise" program for drivers who install a monitoring device onto their vehicle that tracks, and allows for subsequent analysis and sharing of data related to acceleration, time of day driving and other factors deemed relevant (All State Insurance, n.d.).

D. METHODOLOGY

Determining the privacy implications arising from the government's use of sensor technology to monitor the public movement of individuals requires review of law and policy. Therefore, the methodology used in this thesis focuses on legal case and statutory analysis coupled with a comparative analysis of practices regarding the use of various sensor technologies. A review of privacy concepts and how they inform case and statutory law is also conducted. Legal case analysis reviews key judicial decisions regarding technology and privacy, and includes statutory review, where applicable. The purpose of the legal case review is to distinguish and identify the key decisional processes and principles used by the courts to determine the parameters of privacy and technology under Fourth Amendment jurisprudence. Identification of some of the more commonly used sensor technologies within HLS is also conducted. Using the Fourth Amendment and statutory law as a supporting framework, the identification and recommendation of a range of policy options that support public safety and civil liberties, namely privacy, conclude the thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

Several themes evolve from the literature on privacy, technology, and the government's monitoring of the movement of its citizens across public spaces. The first is literature on privacy as a general concept. Literature attempting to define the inherent expectations and legal rights associated with privacy within the United States, both as a theoretical concept and as a legal principle, is also prevalent. A growing body of literature exists on the privacy impact of technology in use within the HLS field. Aggregated data and the subsequent use and retention of mass monitoring data that can be individuated are growing areas of exploration within the literature. In the recent decision in *United States v. Jones*, Justice Sotomayor noted that the use of sensor surveillance technology, inclusive of GPS, provides for a "substantial quantum of intimate information" that bring into question whether it is a reasonable expectation that the sum of an individual's public movements may be tracked for the government to peruse at will (*United States v. Jones*, p. 956), with Justice Sotomayor concurring. While the literature confirms that while privacy is strongly embraced, it often eludes specific definition. Therefore, as a result, privacy will continue to evolve within a world increasingly driven by technology.

A. DEFINING PRIVACY

Privacy represents a panoply of concepts and the literature reflects its broadness of scope and definition. Privacy not only has multiple meanings but the definition has developed over time and is often culturally specific (Gutwirth, 2002, pp. 20, 29). As with fashion, privacy evolves and transforms that which used to be private now publicly acceptable under new standards and vice versa (Baker, 2010, pp. 313–317). For example, as evidenced through reality television shows and social networking, many people are far more comfortable disclosing intimate details about their personal lives than in the past. Whether technology shifts society's privacy expectations, particularly as it applies to legal standards, remains unanswered. Yet, it is society's acceptance of technology, regardless of individual expectations, that forms a critical component in the legal

framework for privacy analysis (*City of Ontario v. Quon*, p. 2629). To date, the U.S. Supreme Court has failed to define the overall extent of technology's impact on reasonable expectations of privacy.

1. Conceptual Privacy

Privacy is often claimed to be a fundamental right (Taylor, 2011, p. 456). However, seemingly little consensus exists as to what is actually being protected (p. 456). Some authors have noted that privacy is inherently rooted in Western culture, with Gutwirth (2002) identifying the challenges in applying Western concepts of privacy, rooted in solitude, to Africa's tribal structure or to some religions, including Islam (pp. 24–29). Others attempt to define privacy within a specific context by identifying salient factors that include normative, social/cultural, and psychological influences (A. Moore, 2008, pp. 411–418; Peters, 1999, pp. 116–118). DeCew (1997) defines privacy, in part, through the analysis of the dichotomy between the public and private realm (p. 9). Adam Moore (2008) identifies that privacy assumes various mores based upon context and situation and is dependent upon cultural boundaries to identify prohibited actions by others, including the government (p. 411). Taylor (2011) argues that space affects privacy, but is not determinative, and, therefore, privacy is retained within public spaces (p. 457). These four factors take on more significance in an age of surveillance technology, where an individual's movements can be measured through GPS for space, time, action, and information. Within the broad realm of the literature on privacy, inclusive of the works of Thomas Locke through Margaret Mead, more than ample support abounds for the existence of the concept of privacy as a matter of natural law, cultural, and political process (DeCew, 1997, chaps. 1–4). Yet, its definition remains elusive, and privacy is subject to individual context and interpretation.

As technology enters the privacy analysis, the literature recognizes the challenge in claiming a right of privacy in public space. Privacy is often seen as "the right to be left alone," the famous opine of Justice Brandeis (Brandeis, 1890, pp. 193–197). However, claims of privacy become enmeshed with digital life, where disclosures of personal and intimate information are voluminous and individual ownership, consent, or control over

PII data becomes increasingly diminished (Nissenbaum, 2000, p. 7). Taylor (2011), in distilling Feldman's communal view of privacy, identifies four dimensions to privacy: space, time, action, and information (p. 457). For some authors, the autonomy of individual decision and control of context defines privacy rather than prohibitions on access to private information (Garfinkel, 2000, p. 4). Peters (1999) argues that the evolving privacy issues within the digital world matter little to real privacy, in that privacy is a state of being, so the digital world has little impact (pp. 117–118). While the collection and retention of individuated information can affect privacy, Gutwirth (2002) notes that such practices have been long standing and existed prior to technology advancements (pp. 16–17). It can be argued that privacy concerns based upon intrusions created by technological advancement are non-existent, and may be based on misinformation and a lack of understanding (Brito, 2004, pp. 19–20). Albeit ephemeral in definition and affected by context, privacy is a well-established concept for review and analysis within the overall literature, at least within the Western culture.

2. Privacy as a Legal Determination

Within the United States, legal decisions and statutory law provide the literature from which the legal concept of privacy is analyzed and defined. In that privacy is evaluated within the lens of cultural, social and technological perspective, McCullagh (2001) argues that privacy definitions and protections are directly correlative to the current views of legislators, judges, and bureaucrats (p. 133). Kerr (2004) identifies that the current legal landscape for privacy relies upon the courts and the Constitution as the primary vehicle for protecting privacy, with Congress and state legislatures having a limited, secondary role (pp. 802–804). Kerr further states that the popular legal view advocates that privacy be advanced by judicial interpretation of the Fourth Amendment to limit the intrusions brought forth by government using surveillance technology (p. 804). However, Heffernan (2001) argues that the judiciary does not have sufficient depth of knowledge to evaluate privacy encroachments fully in light of the current complexity of privacy issues raised by technology (p. 3).

a. Fourth Amendment and Privacy

The literature identifies that, at least within the United States, privacy claims arising under claims from governmental surveillance are inherently linked with the Fourth Amendment to the U.S. Constitution. The Fourth Amendment states: "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 person or things to be seized." (U.S. CONST. Amend. IV). A long line of judicial decisions[9] have established the legal framework for determining whether an impermissible governmental intrusion is occurring under the Fourth Amendment (*Olmstead v. United States*; *Katz v. United States*; *United States v. Knotts*; and *Kyllo v. United States*; *United States v. Jones*). The law has established that individuals do not have a general constitutional right to privacy (*Katz v. United States*). However, the law also states that if the governmental action in question constitutes a search of a person, house, paper, or effect under the Fourth Amendment, then judicial review is warranted to determine whether the government acted in adherence to constitutional principles given the intrusion upon the citizen (*Katz v. United States*; *Kyllo v. United States*).

(1) Search and Reasonable Expectations of Privacy. The literature identifies that not every government intrusion is a search (*Oliver v. United States*).[10] Judicial interpretation of the term "search" is not only sometimes inconsistent with its popular use within the lay population; it is subject to varying judicial definition (Hutchins, 2007, p. 422). Even if it is determined that a search occurred, the courts must

[9] Case law serves as the "literature" for legal analysis, and is defined as "the aggregate of reported cases as forming a body of jurisprudence, or the law of a particular subject, as evidenced or formed by the adjudged cases, in distinction to statutes..." (Black's Law Dictionary, 1979).

[10] In *Oliver*, the U.S. Supreme Court held that government's search of a field removed some distance from the defendant's home was not a search under the Fourth Amendment, thereby reaffirming the open fields doctrine, under which there is no reasonable expectation of privacy in open fields, despite an individual's attempts to limit access (*Oliver v. United States*, p. 178).

still determine whether the individual had a reasonable expectation of privacy and, if so, whether the individual privacy interests were objectively reasonable (Hutchins, 2010, pp. 1191–1192).

Katz (*Katz v. United States*) identifies that location is not the sole driver for reasonable expectations of privacy, as the Fourth Amendment protects people and not places (p. 351). However, trespass by the government remains a key factor under the reasonable expectation of privacy analysis, even in an age of technology, as evidenced in its most recent decision in *Jones.* Rather than address the issues associated with mass surveillance by the government through use of GPS, the Supreme Court focused on the government's physical trespass to install the GPS device in holding that the government had conducted a search for Fourth Amendment purposes (*United States v. Jones*, pp. 948–950).

Gershman (2010) maintains that "place" remains a central issue in determining reasonable expectations of privacy, as demonstrated in the *Katz* court's focus on the use of surveillance to listen into a conversation from within a phone booth (p. 928). Given the traditional focus on physical entry as a predicate for a finding of a search, at least in conjunction with a reasonable expectation of privacy, Kerr (2005) questions what would constitute a search when a computer storage device or its data is involved (pp. 538–539). Kerr further discusses the challenges of place, such as in distinguishing what is a "home," the traditional privacy boundary, in an electronic age where many private effects are now portable (p. 538).

Other authors also identify that the existing analytical framework and legal theory of the Fourth Amendment, particularly as it applies to technology, is confusing and inconsistent (Recent Cases, 2011a, pp. 832–834; Plourde-Cole, 2010, pp. 579–582). Cloud (2002) finds that the *Katz* standard of reasonable expectation of privacy fails when applied to surveillance technologies (pp. 28–29).

Justice Alito argues that technical trespass, the basis for decision in *Jones*, is a step back in the privacy jurisprudence (*United States v. Jones*, p. 960), with Justice Alito concurring. He further observes that the majority fails to follow its own

precedence, as decided in *Kyllo*, in which the Court recognized that the Fourth Amendment does not require physical trespass, and in *Katz*, in which the Court identified that the existence of a property right is but one element is establishing a reasonable expectation of privacy (p. 960).

Clancy (2012) argues it is almost impossible to identify exactly what the concept of a reasonable expectation of privacy means under existing legal jurisprudence (p. 303). Hutchins (2007) puts forth the idea that the Supreme Court's interpretation of the Fourth Amendment analysis has been erratic and occasionally contradictory (p. 422). Gershman (2010) identifies that the factors used by the courts in determining reasonable expectations vary on their face (pp. 928–929). Given the circular analysis required under the *Katz* standard of reasonable expectation of privacy—as the two pronged test to determine a reasonable expectation of privacy requires both the subjective and societal privacy expectations be met for a privacy claim to be deemed reasonable—the literature lacks consistency in defining what is required to assert a claim of privacy properly under the Fourth Amendment.

Under the reasonable expectation of privacy standard, the literature discusses whether length and duration of the government intrusion contributes to the finding that the government action was a search. Solove (2004) identifies that much of the 4th Amendment jurisprudence focuses on a search as a physical incursion (pp. 196–197). Gersham (2010) identifies that modern technology enables the government to intrude into places and activities that previously were inaccessible, and the courts have yet to address the issue under a reasonable expectation of privacy analysis (pp. 928–929). Kerr (2011) posits that given a government search is defined as a discrete act, legal determinations based upon the duration of the act, including the continuing delivery of information arising from the act, should not define whether a search occurred. Alternatively, Kerrane (2011) argues that with GPS, the ability to capture large amounts of information via constant satellite monitoring should impact determinations of whether a search has occurred for Fourth Amendment purposes (pp. 1734–1741). Therefore, when technology is involved, the legal literature differs as to what specific factors are determinative of whether a search occurred, be it physical intrusion, duration or degree of

intrusiveness (Hutchins, 2010, pp. 1185–1190; Plourde-Cole, 2010, pp. 571–627; Wells, 2009, p. 225; Koppel, 2010, pp. 1069–1073). As technology is able to obtain greater stores of information with minimal physical intrusion or awareness by the individual under surveillance, the debate over the degree of governmental intrusion will become less relevant.

(2) Reasonable Expectations of Privacy. The expectation of privacy is a two-pronged test, inclusive of a subjective expectation of privacy, where an individual exhibits an actual expectation of privacy, and the second prong, a requirement that society is prepared to recognize the expectation as reasonable (*Katz v. United States*, pp. 347, 361). Objective societal expectations have been defined as those expectations that drive the "normal course of business" or information that is voluntarily and/or routinely disclosed (*Smith v. Maryland*). Within the context of reasonableness, the courts have recognized that although a person voluntarily exposes their daily movement and actions in public, a person does not leave his privacy home upon exiting the door (*United States v. Maynard*, p. 563).[11]

The literature identifies that evolving technology presents challenges to identifying societal expectations of privacy. Slogobin (1993) identifies that the Court relies upon societal understandings of privacy in defining legitimate expectations of privacy under the Fourth Amendment (p. 731). With technology in play, Freiwald (2007) states the courts lack the competence to evaluate societies' views about the intricacies of technology and its application, as most users and judges do not fully understand new technology (p. 8). Even the Supreme Court itself has acknowledged that *Katz* test has been criticized as circular, and hence subjective and unpredictable (*Kyllo v. United States*, p. 34). Further, the U.S. Supreme Court has noted that the reasonable expectation of privacy analysis requires an underlying expectation that the reasonable person has a well-developed and stable set of privacy expectations (*United States v. Jones*, p. 932), with Justice Alito concurring. However, expectations of privacy are subject to significant flux during times of dramatic technological advancement (p. 932).

[11] Maynard is the D.C. circuit court decision that is subsequently renamed and decided by the U.S. Supreme Court in Jones v. United States. See footnote 17.

Given the ongoing dramatic changes in technology, the literature does discuss that the judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clearly understood and accepted, and embraced under reasonable expectations of privacy (*City of Ontario v. Quon*, p. 2629). Within the literature, there a public reserve for privacy is recognized. However, whether subjective expectations of privacy remain objectively reasonable is influenced by society's acceptance and understanding of the overall use of technology.

The dicta of the court, as expressed through concurring and dissenting opinions that attach to judicial decisions, also expands the literature on legal interpretation of the privacy protections afforded U.S. citizens under the Fourth Amendment and the reasonable expectation of privacy doctrine. For example, while the Supreme Court's decision in Jones decision was unanimous, meaning that all the justices concurred that the government engaged in a search for Fourth Amendment purposes, the basis for the opinions varied (*United States v. Jones*, p. 945). The majority[12] in *Jones* held that the government engaged in trespass by placing a GPS device on the subject's vehicle, and therefore, was search under the Fourth Amendment (p. 954). However, the majority chose not to address whether the use of GPS for a period of 28 days without a warrant violated the reasonable expectation of privacy under the Fourth Amendment, finding it unnecessary to do so given the governmental trespass (p. 950). While Justice Sotomayor concurred that trespass did in fact give rise to the finding of a search for constitutional purposes, she gave separate voice, in her concurring opinion, to the unease surrounding the growing privacy concerns and impact on the relationship of government to its citizens in light of advancing surveillance technology (pp. 954–956). The remaining Supreme Court justices, while concurring with the finding that the government engaged in a search under the Fourth Amendment, disagreed as to the majority's reliance upon the trespass doctrine (*United States v. Jones*), with Justice Alito concurring (pp. 961–963). Rather, Justices Alito, Ginsberg, Breyer and Kagan all concur in the finding, but identify

[12] The majority comprised of Justices Scalia, who delivered the opinion of the Court, and Justices Roberts, Kennedy, Thomas and Sotomayor. Justice Sotomayor also filed a concurring opinion. Justice Alito also filed an opinion concurring in the judgment, in which Justices Ginsburg, Breyer and Kagan joined (*United States v. Jones*, p. 947).

that for most offenses, longer term use of GPS monitoring impinges on reasonable expectations of privacy. See *United States v. Jones*, with Justice Alito concurring (p. 964). Therefore, while the decision in *Jones* is unanimous, a review of the contributing opinions identifies distinct lines of support for the decision.

The *Jones'* opinion will contribute to the ongoing legal discussion during subsequent judicial review of claims of Fourth Amendment violations arising out of the government's use of GPS, as well as other sensor technology, to conduct surveillance. In that the determinations of whether a reasonable expectation of privacy is factually driven and is subject to the privacy hermeneutic of the deciding judge, (as well as proficiency with modern technology), the case law will always show some level of variance in the analysis of distinct technologies and their privacy impacts. However, the law's capacity to address the privacy impact of new technology occurs through the lens of socially accepted uses of technology and the dynamics of communication and information transmission (*City of Ontario v. Quon*, p. 2629). As a result, the literature identifies that the expanding use of technology becomes part of the fact pattern for Fourth Amendment analysis in determining both subjective and reasonable expectations of privacy, which serves to add to the confusion over the proper use of technology in conducting mass surveillance.

(3) Other Legal Privacy Protections. The legal literature on privacy also derives from a wide variety of statutes that address privacy at both the state and federal levels. Legal statutes are the result of legislative action, as opposed to case law that arises out of judicial decision. Solove (2010) identifies that legislative bodies are the more appropriate conduit for delineating rules for government information gathering and the courts are best situated to evaluate whether these rules meet the basic principles of the Fourth Amendment (p. 1538). Unlike the Fourth Amendment, statutory provisions to protect privacy interests may also regulate the activities of private individuals.

(4) Federal Statutes. The literature review identifies that a general right of privacy does not exist in either constitutional or statutory law within the United States (Stanley & Steinhardt, 2003, p. 15). Various federal laws address privacy by limiting the context in which government, and some private entities, may access

information deemed private. For example, the Gramm-Leach-Bliley Act, which regulates the sharing of PII financial information about individuals engaged in business with data collectors (Gramm–Leach–Bliley Act (GLBA). Video records are protected through The Video Privacy Protection Act of 1988 (codified at 18 U.S.C. § 2710 (2002) The Health Insurance Portability and Accountability Act (HIPAA) defines and limits how government and private entities access and disseminate individual health care information (The Health Insurance Portability and Accountability Act, 1996). Consistent with the examples provided by these laws, statutorily mandated privacy protections are generally of limited scope and application, often focusing on a specific area of the law or issue.

Some generalized data protections exist at the federal level for PII data under government access and control, although they also are limited in overall scope and application. The Privacy Act of 1974 governs the maintenance and disclosure of PII records maintained by federal governmental agencies (The Privacy Act of 1974, as amended 5 U.S.C. § 552a). The U.S. Code of Federal Regulations, 28 Code of Federal Regulations (CFR) Part 23, acts as a guideline for standards on the collection and use of criminal intelligence, inclusive of PII for federally grant-funded multijurisdictional criminal intelligence systems (Institute for Intergovernmental Research, n.d.). However, the literature identifies that not all data is subject to statutory restrictions, and the depth of information about individuals held by the federal government creates privacy concerns given the relatively easy access to data and the subsequent ability to aggregate data (Gross & Inkley, 2005).

The literature identifies that federal statutory control over technology and practices used by local law enforcement to conduct surveillance is limited. One notable exception is the Title III of the Omnibus Crime Control and Safe Streets Act of 1968, (“Title III”), which regulates wiretap surveillance of communications for both federal and local law enforcement (18 U.S.C. §§ 2510–2522). Title III provides for a limited grant of authority to law enforcement for electronic surveillance for specifically delineated crimes and only in accordance with certain procedural requirements as listed under 18 U.S.C. § 2516(1). Statutory law, rather than constitutional protections, provides the better legal privacy protection from governmental

wiretapping surveillance (Kerr, 2004, p. 850). The U.S. Supreme Court has noted that in enacting Title III, Congress ensured that the complex field of electronic surveillance was not left to the courts to govern through evolving case law (*United States v. Jones*, p. 963). However, Title III is limited in its privacy protections as it addresses only specified eavesdropping technology in use by the government, and not others, inclusive of GPS (*United States v. Torres*, p. 884). The literature identifies that other federal statutory limitations exist, for example, through components of Title III, such as the Stored Communications Act (18 U.S.C. §§ 2701–2712), or through the Electronic Communications Privacy Act of 1986, (ECPA), (18U.S.C.§2510–2522, Pub. L .99–508). However, the literature does not identify a similar federal jurisdictional reserve as is seen in Title III, which illuminates both the gap in privacy as a result of anemic statutory privacy laws and the ability of such legislative action to provide comprehensive legal protections.

b. Privacy under State Law

State and other local law has a growing impact on individual privacy protection as it relates to the use of technology, although little consistency or shared policy focus exists amongst the states. The Supreme Court has ruled that the protection of a person's general right to privacy, inclusive of the right to be left alone, is similar to the protection property and life, and therefore, is a responsibility of the states (*Katz v. United States*, pp. 350–351). While a variety of local law addressing private information and its protection exists, a literature review identifies that no single state has a comprehensive privacy protection statute. Some states provide constitutional protections for general human rights and privacy. For example, the Florida Constitution provides that "Every natural person has the right to be left alone and free from governmental intrusion into the person's private life except as otherwise provided herein (Florida State Constitution, art. 1. sec. 23). The State Constitution of Alaska recognizes a right of privacy for people and states that it shall not be infringed (Alaska State Constitution, art. 1, sec. 22). Some states, like Hawaii, recognize a right of privacy, but limit its protections if a compelling

government interest driving the intrusion exists (Hawaii Constitution, art. 1, sec. 6). Therefore, while the federal constitution remains silent on the issue, some states have identified privacy as an inherent right within their constitutions.

The literature reflects that Freedom of Information Act laws (FOIA) and sunshine laws also affect privacy. The literature identifies that given concerns over growing government bureaucracy and secrecy, FOIA was the legislative response to ensure an open government with appropriate public access (Wichmann, 1998, pp. 1217–1218). However, technology brings forth voluminous amounts of data and at least one author has questioned whether public records, which contain significant amounts of PII data, were meant to be public to the degree enabled by technology (Salzmann, 2000, p. 356). Regardless of legislative intent, state level FOIA laws increasingly define privacy, given the mandated disclosure of data under the FOIA goals of openness, without legal consensus as to what is appropriately identified as PII and disclosed within the context of privacy (p. 379).

In the absence of federal statutory preemption or a comprehensive Supreme Court decision on privacy, local and state governments are increasingly establishing their own legal parameters for the use of surveillance technology. However, the privacy policies of the varying states may conflict with one another. The literature identifies that some state courts, including Washington, Delaware, New York, and Massachusetts, require law enforcement officers to obtain a warrant before using GPS surveillance, absent exigency (Smith, 2011, p. 7). Other state courts, including those of Nevada and Virginia, have found that use of GPS surveillance does not constitute a search, and therefore, does not raise any state or federal constitutional concerns (p. 7). Other states, including California, have statutorily limited the right to track a person electronically to law enforcement, and identifies that doing so without a person's knowledge is a violation of reasonable expectations of privacy. See, e.g., California Penal Code section 637.7, Stats. 1998 c. 449 (S.B. 1667) § 2. The emerging body of local privacy laws applicable to the government's use of surveillance technology is varied and does not reflect a unified policy vision for privacy.

The literature notes increased reliance upon state law in protecting the privacy interests of its citizens. Gersham (2010) has noted that the expectation of privacy jurisprudence from the U.S. Supreme Court is confusing (p. 929). As a result, Gersham argues that the lack of legal consistency has encouraged state courts to reject the *Katz* doctrine and to provide broader protection to its citizens under the state's law (p. 929). For example, the Washington State Supreme Court has held that a right to privacy is one of conscious decision and to define privacy through the capacity of current technology is inconsistent with state constitutional privacy protections and fails to guide proper governmental action (*State v. Young*, p. 598). The issue before the court was whether the use of a thermal imaging device to obtain information from within the home of a suspected marijuana grower was a search under the Fourth Amendment (p. 594). In ruling that the government's action was an impermissible search, the court held that an "even more rigorous protection of privacy" exists under the state constitution than under the Fourth Amendment (pp. 596–598).[13]

Another example of local law providing rights not specifically delineated in federal law occurs in *Commonwealth v. Connolly* (*Commonwealth v. Connolly*). The issue before the Supreme Court of Massachusetts was whether the use of GPS by law enforcement to conduct warrantless surveillance was illegal (*Commonwealth v. Connolly*). Relying upon the protection under Article 14 of the Massachusetts Declaration of Rights, which grants the right to be secure from all unreasonable searches, and seizures absent proper warrant, the court found an impermissible search occurred (*Commonwealth v. Connolly*, p. 369). In addressing the government's claims that no Fourth Amendment right to privacy exists regarding a vehicle's movement about the public way, the court held that the state law provides protection at least equal to, and at times greater than, that provided by the Fourth Amendment, and that the installation of the GPS device constituted a seizure under the state law (*Commonwealth v. Connolly*). The legal literature reflects the variance in the local protections for privacy among the states. This

[13] This 1994 decision predated the U.S. Supreme Court's decision on a similar use of the technology in *Kyllo v. U.S.* in 2001. The U.S. Supreme Court decided along similar lines in its decision in *Kyllo*, finding that the use of an infrared imaging device to obtain information from inside the home was a search under the Fourth Amendment (*Kyllo v. United States*).

variance has negative impact on the government's ability to conduct criminal investigative surveillance, which in terms, limits individual privacy rights in that privacy protections become a matter of jurisdictional border and not consistent public policy.

(1) Comparative Law. The literature identifies that legal privacy protections within the United States are anemic in comparison to those of its European counterparts. From the perspective of PII, Bergelson (2003) states that within the United States, comprehensive legislation regulating the privacy rights and responsibilities of individuals and commercial enterprises that collect PII is needed due to the development of privacy laws in the international arena (pp. 394–395). Many European countries,[14] including members of the European Union (EU), offer specific, enumerated privacy protections for their citizens. Those countries with delineated privacy protections under law include, but are not limited to Belgium, Brazil, Finland, Greece, Israel, Italy, Spain, and Sweden (Privacy International, 2007).

One significant vehicle driving privacy rights is the European Convention of Human Rights (ECHR).[15] Bignami (2007) states that while the European Union is not a party to the ECHR, both treaty and case law establish that ECHR rights are guaranteed to citizens within the European Union (p. 241). Morariu (2009) identifies that while Article 8 of the ECHR guarantees the right to private life and family life, it also provides for restrictions of this right under certain circumstances (p. 47). Taylor (2011) argues that privacy rights are not absolute and that proportionality, a recurring theme under European law, is focused on maintaining the contextual integrity of individual privacy in light of governmental surveillance (p. 460). The examination of the balance between societal rights and personal privacy protections is a recurrent theme within some of the EU literature and discussion on privacy.

Beyond general privacy principles, Bignami (2007) identifies that within the European Union, data protection is treated as a basic human right (p. 233). The literature notes that data protection acts regulate the retention and use of derivative data

[14] This thesis focuses on European countries given the shared democratic principles and general legal concepts with those of the United States.

[15] The Council of Europe includes 47 member countries and seeks to develop common principles based on the ECHR in the protection of individuals (Council of Europe, n.d.).

and not a specific technology or interest area. For example, The Data Retention Directive, (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006), provides for a variety of protections associated with the collection and transmission of PII and data transmitted through electronic means (See Article 4 and Article 5). Elaluf states that data privacy laws are privacy driven, and not focused on a specific technology and therefore are seen as technology neutral (Elaluf-Calderwood, Hosein, Karrberg, & Liebenau, 2011, p. 6). Overall, the literature identifies that EU data protection laws focus on the individual/societal privacy interest rather than a specific technology in making privacy determinations.

Technology use also drives privacy definitions and protections within the European Union. The evolution of the use of CCTV within the United Kingdom is a good example of how the privacy issues brought forth through the government's use of technology to conduct surveillance help to further define privacy standards. The literature identifies that as a result of a legal gap in the early stages of the U.K.'s implementation of CCTV, surveillance occurred with minimal regulation (Zoufal, 2008, p. 129). Zoufal states that as co-regulation evolved, self-regulation with government and private sector involvement, also helped establish privacy standards for the U.K.'s use of CCTV (p. 129). For Webster (2004), the lack of formal legislation governing CCTV is seen as opening the way for the development of voluntary codes of practice, which in turn, fed the emerging legal standards for CCTV implementation (pp. 231–232). These emerging U.K. legal standards, according to Taylor (2002), included protecting the individual's privacy right not only in the initial collection of sensor data, but also in the subsequent dissemination of data captured via surveillance (pp. 76–78). In guiding determinations about use and dissemination regarding surveillance data, Taylor (2011) states that the law becomes a means to protect privacy by identifying when the privacy interest is substantial enough to demand state action rather than state neutrality (p. 457). The literature review reveals that no encompassing federal statute regulating general rights of individual privacy or data protection exists in a manner comparative to that seen within many European nations.

B. PUBLIC POLICY AND TECHNOLOGY

While technology is inanimate, its use by government is not and the literature not only evaluates the capacity of technology, it explores the policy implications of the government's use of surveillance technologies. Taylor (2002) notes that surveillance generally has two faces, that which intrudes upon or curtails privacy rights, and that which pre-empts crime and protects the public (p. 66). Garfinkel (2000) notes that technology development and its use do not occur in a vacuum, but that public choice and politics also have a role in defining rights and expectations around technology use (p. 11). Although the science of sensor technology is not a focus of this thesis, aspects of the science do impact the discussion on privacy, particularly as to the reliability of the science behind evolving technology. Technical literature covers the realm of sensor technology used in support of HLS interests, with some recognition of the inherent privacy concerns brought forth by the use of sensor technology to conduct surveillance. See Introna and Nissenbaum (2009, pp. 44–46) for a discussion on alleviating privacy concerns over the use of FRT. The literature on the privacy impact of the government's use of surveillance technology often results in use and/or policy recommendations.

A variety of authors weigh in on evaluation and policy recommendations concerning the government's use of surveillance technologies. Civil liberties groups, such as the American Civil Liberties Union (ACLU), contribute to the literature through analysis of certain technologies resulting in policy recommendations for the government's use of sensor technology generally more restrictive given identified privacy and other constitutional concerns. The ACLU maintains a website, Spy Files,[16] which catalogues many privacy issues associated with surveillance technology. Literature from civil liberties advocates generally favors reduced reliance upon and greater controls over the government's use of sensor technology.[17]

[16] See the ACLU website for a variety of issues and concerns over governmental surveillance (Spy Files, n.d.).

[17] For example, see the website for the Northern California ACLU, "Connecting the Dots" (Connecting the Dots, n.d.).

The literature generated by governmental agencies and those generally associated with the government tend to focus on technology performance and its efficiencies, and often provide recommendations for reducing privacy impact. For example, technical literature, such as that written by the National Science and Technology Council (NSTC) (2006), analyzes the performance of the underlying biometrics technology, and also identifies privacy concerns with recommendations for policy (pp. 43–57). The International Association of Chiefs of Police's (IACP) (2009) report on the privacy impact of LPR analyzes not only the key components and use of the technology, but also identifies privacy concerns and makes recommendation for policy so that law enforcement can reduce the privacy concerns.

Literature also evaluates technology, from the general evaluation of efficacy, to the impact on specific privacy concerns that the different types of technology bring forward. While the science informing sensor technology is not a focus of this thesis, the science does impact aspects of privacy, and therefore, some of the literature remains relevant. The literature is informed by academic articles regarding the science behind the technology, such as evaluation and validation of the underlying algorithms for LPR (Obeid et al., 2007). Government sponsored evaluation of technology is another source of literature, such as the review and measurement of FRT improvement over time, inclusive of comparison among specific vendors (Phillips, Scruggs, O'Toole, Flynn, Bowyer, Schott, & Sharpe, 2007). Even the literature on scientific validation of the technology is cognizant of privacy concerns linked to surveillance technology. The NSTC Subcommittee on Biometrics provided analysis of existing biometrics and associated public policy concerns for use, both front and end use, of the data collected—including collection, storage and comparison (NSTC, 2006). Introna provides an analysis of the efficacy of FRT technology, gives policy considerations informed by the technology requirements and limitations and identifies the resulting impact on privacy concerns associated with FRT (Introna & Nissenbaum, 2009). The technology evaluation literature informs as to the capacity of the technology, as well as its resulting privacy impact.

Civil liberty advocates are generally more focused on the resulting privacy impact of technology. The ACLU has contributed much to the literature on the privacy impact of

technology, including technology evaluations and policy recommendations that strongly advocate for enhancing privacy protections within existing surveillance systems (Ozer & Schlosberg, 2007; Chicago's Video Surveillance Cameras, 2011). Cameron (2008) studied the use of video surveillance within the Los Angeles area and identified the strengths and limitations of the technology and the policies in use by law enforcement (p. 53). Other literature calls for a moratorium on the expansion of video surveillance by citing the need for an open evaluation before the government chills expressive freedom (Chicago's Video Surveillance Cameras, 2011, pp. 1–3). The ACLU of Northern California identifies that video surveillance has not proven effective and that government should pause on the implementation to determine whether funding would be better spent elsewhere (Ozer & Schlosberg, 2007, p. 2). The literature, therefore, covers a range of issues in regards to the technology itself, from the scientific underpinnings to how the technology creates privacy concerns to drafting policies to address or limit such concerns.

1. Legal Impact of Technology

Some legal-based literature examines surveillance technology used by the government and its impact on privacy from a legal perspective. Well before the expansive reach of modern technology, Justice Brandeis noted that technology allows the government to invade privacy in a manner equivalent to, or even more far reaching, than any physical intrusion (*Olmstead v. United States*, pp. 472–473). Zoufal (2008) notes that even court decisions involving analogous technology often result in disparate judicial outcomes (pp. 103–105). For example, Plourde-Cole (2010) identifies that despite similar technologies, the law has yet to link consistent legal theory to the privacy impact of cell phone tracking and GPS tracking (p. 575). Zoufal (2008) identifies that disparate legal outcomes are rooted in a judicial privacy analysis specific to the technology in use and not to general privacy implications (p. 104). Freiwald (2007) argues that the courts are incapable of tackling the challenges of technology and that the *Katz* test fails to provide for any consistent direction in evaluating the privacy impact of technology. As the literature demonstrates, the technology itself continues to play a key role in determining whether the government's use of certain technology in fact triggers statutory or Constitutional protections.

Some authors have argued that the legal jurisprudence under the Fourth Amendment is either inapplicable or flawed in regards to today's digital world. Solove (2006b) argues that a new taxonomy is needed for privacy to be protected within the United States as the Fourth Amendment simply does not work in protecting privacy given the advancements of technology. For McCullagh (2001), technology and its impact on privacy cannot be properly addressed within the law, but, rather, is a market issue that will increase or decrease depending upon the privacy values identified within the society (pp. 129–131). In McCullagh's market driven privacy protections, as technology advances, individuals are free to develop and use technology to diminish the negative privacy impact brought forth using technology (pp. 129–131). The law is merely a secondary vehicle in protecting privacy.

Privacy as a function of capitalism is also discussed within the literature under the umbrella of data aggregation. Garfinkel (2000) identifies an Orwellian world in which privacy, by means of aggregated data, is forfeited not as a result of government control, but rather as an outgrowth of capitalism and societal priorities (p. 2). Peters (1999) identifies that businesses, rather than just government, also have a vested interest in computerized monitoring and the aggregated data that results (p. 57). Scott (2012) puts forth a consumer driven theory of privacy. He uses Facebook's reference ads for third party websites that deliver targeted advertising to Facebook consumer's home pages, as an example, and notes that such policies are driven by the company's ability to mine and use the data content on Facebook user's pages (Scott, 2012).

Conversely, other authors find that the existing legal framework to protect privacy rights is up to the challenge brought forth by modern technology (Brandeis & Warren, 1890, pp. 193–195). Kerr (2004) favors the primacy of the Fourth Amendment for limiting privacy encroachments caused by the government's use of surveillance technology, which is the popular legal view (pp. 802–804). He advocates that when technology threatens privacy, the courts and the Constitution should be the primary response. Given the reliance upon precedence within the U.S. legal system, much of the

existing legal literature, inclusive of the recent U.S. Supreme Court decision in *Jones*, is founded upon the existing Fourth Amendment framework in determining the privacy rights of individuals given the government's use of surveillance technology.

C. MINDING THE GAP

How technology impacts legal determinations of privacy is another theme in the overall literature. Despite the prevalence of surveillance technologies in use by private, commercial, and government actors, the literature generally reflects a greater focus on the privacy impact resulting from the government's use of sensor technologies (Brito, 2004, pp. 30–33). The literature reveals an active debate as to what is the appropriate legal nexus between privacy and the government's use of surveillance technology.

Justice Brandeis' dissent in *Olmstead* argued that evolving technology allows the government to be less intrusive when entering into the private realms of its citizens (*Olmstead v. United States*, pp. 471–485). His focus of concern still remains a valid legal issue. As technology continues to advance, some authors, including Posen, have noted that new technologies generate greater concerns for individual privacy in light of the risk of disclosure that massive data collection brings (Posen, 2005, p. 632). However, Solove (2006b) puts forth that it is not technology, but rather, the activities of people that erode privacy (p. 564). Solove states that the way to protect privacy is for the courts and legislatures to regulate the activities of people and not the technology (p. 564). Zoufal (2008) finds that while modern technology generates privacy concerns, legal privacy protections are well established under U.S. law (pp. 156–159). Accordingly, privacy will not be destroyed or impacted by technology to the degree claimed by privacy advocates (pp. 156–159).

Conversely, Clancy (2012) argues that the U.S. Supreme Court's decision in *Jones* merely recycles old law regarding property versus privacy, and the law does not adequately confront the privacy issues of the digital age (p. 303). Given the adherence to precedence under case law, Hutchins (2010) notes that decisions involving earlier technology determine the tolerance for future technologies, but the older decisions fail to address or account for the greater intrusions brought forth by modern technology (p.

1187). Solove (2006b) posits that "abstract incantations of privacy" are not nuanced enough to capture the practical and intricate problems involved with the governmental use of surveillance technology and its impact on privacy (p. 480).

The retention and aggregation of data is the new privacy frontier. Earlier literature regarding privacy and technology is often focused on how the technology facilitated or enhanced observation. For example, in *Kyllo*, the U.S. Supreme court analyzed the privacy implications under the Fourth Amendment when the government used infrared technology to conduct surveillance into an individual's home, but was focused on the issue of observation and not necessarily collection[18] (*Kyllo v. United States*, p. 27). However, as the government's use of sensor technology to conduct surveillance continues to grow, the literature reveals increasing concerns over privacy protections as they apply to the government's back end collection and retention of data (Sanchez, 2010). As Solove (2010) notes, individuals may not have a concern in disclosing relatively small amounts of PII data, but with modern surveillance technology, smaller amounts of PII data can be combined, and thus create an aggregation effect that provides a far more comprehensive picture of the individual than the discrete dataset deemed acceptably disclosed (p. 1523). The literature is beginning to focus more on the aggregation use of the data captured through government's use of surveillance technology, as opposed to just the initial observation. Whether the concerns over technology's impact on privacy and the availability of aggregated, individuated data is a real or inflated concern remains subject to ongoing debate within the literature.

Judicial decisions are also beginning to note the privacy concerns generated by the aggregated data that results from the government's use of surveillance technology. In *United States v. Maynard*, the court discusses the Mosaic Theory—the amassing of individual, discrete data such that a broader, more descriptive, and therefore intrusive, set

[18] In *Kyllo*, the U.S. Supreme Court opened the door to the issue of whether technology that is widely available, "in general public use" can impact privacy expectations, in ruling that the use of infrared technology to conduct a search of a home interior was a search for Fourth Amendment purposes, in part because the technology used was not in general public use (*Kyllo v. United States*, p. 28).

of data results (pp. 561–562).[19] The *Maynard* court found the level of data collected through GPS surveillance to be of significant concern for privacy. (pp. 561–562). The *Maynard* court identified that the continual surveillance of a person's every movement over a period of 28 days was not "knowingly" exposed to the public, as little likelihood existed that anyone would view all movement (p. 558). The court went further and stated that the ability of GPS to capture the whole of an individual's movements, rather than distinct parts, did not result in a constructive exposure as a person would not reasonably expect such action, and therefore, the government's use of a GPS tracking device in this manner was a search for Fourth Amendment purposes (pp. 561–562). In a New York state court decision, *People v. Weaver*, the court found that GPS is a vastly different and exponentially more sophisticated technology easily and cheaply deployed with virtually unlimited and remarkably precise tracking capability (p. 1199). The *Weaver* court held that because of the detailed information collected by a GPS tracking system, significant privacy concerns are created, and therefore, legal protections attach. The split in decisions among the lower courts contributes to the overall uncertainty relative to the proper use of surveillance technology by the government.

The Supreme Court has not provided guidance on privacy standards associated with the mosaic theory or aggregated data, despite opportunities to do so, even as recently as its decision in *Jones* (*United States v. Jones*, p. 948). As such, given the reliance upon *stare decisis* within the U.S. courts, PII and data aggregation privacy protection remains, for the most part, a matter of statutory regulation. The literature shows that the U.S. Supreme Court favors state regulation, as opposed to constitutional review, of privacy data that arises as a result of technology advancements (*Whalen v. Roe*, pp. 605–607).

1. Impact

The literature brings forth concerns over the potential for misuse and abuse of the secondary data derived from the use of sensor technology to conduct surveillance. The

[19] *U.S. v. Jones* was a consolidated case, originally named *U.S. v. Maynard*. However, the conviction of the defendant Maynard was upheld by the D.C. Circuit Court of Appeals while the defendant Jones' conviction was overturned as a result of the GPS claim. The government sought writ of certiorari from the U.S. Supreme Court only as to *Jones* and the issue of whether GPS is a search for Fourth Amendment purposes.

literature also discusses not only the capacity for enhanced data aggregation that technology brings forth, but also the individuated detail that becomes accessible through larger databases (Zoufal, 2008, p. 113; Guidelines for Public Video Surveillance, 2007, pp. 1–6). Concerns are raised about the potentially chilling effect on civil liberties, which arise out of the ability of government to influence individual conduct or ignore individual constitutional rights improperly because of data collection practices (National Research Council of the National Academies, 2008, pp. 3–4). Most recently, Justice Sotomayor noted that government surveillance may chill associational and expressive freedoms, and the unrestrained power to aggregate the data obtained is susceptible to abuse (*United States v. Jones*, p. 956).

However, DeCew (1997) identifies that value does exist in government surveillance as a means to end crime and posits that technology and privacy are not antithetical to one another (p. 163). Introna recommends that governmental policies and practices need to evaluate and address technology's capacity to gather significant amounts of data (Introna & Nissenbaum, 2009, p. 5). Garfinkel (2000) goes one step further by claiming that the government may be the best option to protect privacy (p. 6). Kerr (2011) challenges whether the mosaic theory has any relevance in Fourth Amendment jurisprudence and argues that the Fourth Amendment is discreet and applies only to searches and/or seizures. Under the mosaic theory, Kerr (2011) argues that any attempt to make that which is not a search a search if information is grouped in a particular way has no appropriate standing under Fourth Amendment law. For Kerr, it is or is not a search, and the degree of governmental intrusion is irrelevant in making the determination. The literature reflects that as data becomes increasingly digitized, and more easily accessed and associated, concerns about data accuracy and the subsequent use and impact of individuated data grows.

2. Conclusion

The use of technology and sensors to conduct surveillance continues to expand rapidly, as does its use within the HLS field. A vast amount of literature covers privacy, technology, and the ensuing implications for civil liberties. Surprisingly, no single

definition of privacy exists within the literature. Not as surprising, this gap translates, in part, to varied and sometimes contradicting legal definition and privacy analysis by the legal system, particularly under the Fourth Amendment. As the literature reflects, the rapid growth in technology, as compared to the relatively slow evolution of privacy law, creates a gap in not only legal structure, but also in defining the boundaries of privacy and government policy relative to the collection and use of PII and personal data overall.

III. THE INTERSECTION OF PRIVACY AND TECHNOLOGY

A. PRIVACY

> That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection.
>
> – Justice Brandeis, U.S. Supreme Court, 1890

> You have zero privacy anyway. Get over it.
>
> – Scott McNealy, Sun MicroSystems Co-Founder, 1999
> (quoted in Schwartz, 2001)

The explosive growth of governmental surveillance technology to track the movement of individuals within public spaces has served to elevate civil liberties and privacy concerns. Defining privacy is critical to the legal framework that ensures the civil liberties granted to American citizens. As it applies to the government's use of sensor technology to monitor the public movement of its citizens, it becomes an issue of relativity—what is private within the public arena? However, what privacy means in a world in which a variety of technology can continuously monitor individuals and their movement across public spaces has yet to be adequately defined, through either law or culture. Government and its citizens continue to grapple with defining privacy in an age of CCTV, GPS, sensor technology, smart phones, Facebook, Twitter, YouTube, and client loyalty registrations. Given the growing web of digital immersion, the privacy debate has been energized because what is "public," and therefore not private, is undergoing a sea of change within modern society (Garfinkel, 2000, ch. 5). As such, the courts are left to interpret the cultural context afforded privacy in a rapidly evolving technological world. Absent sufficient definition and structure, the law cannot give full effect to privacy protections, subjective or objective.

1. Defining Privacy

Privacy reflects a "penumbra of rights and expectations" (*Griswold v. Connecticut*, p. 483). From a practical perspective, privacy is an umbrella term covering a

disparate range of concepts (Solove, 2006b, p. 483). Yet, little consensus exists as to what is actually being protected under the claims of a fundamental right of privacy (Taylor, 2011, p. 456). Webster's definition of privacy hits three key concepts: seclusion, freedom from unwarranted intrusion, and secrecy (Merriam Webster, n.d.). Privacy has no single meaning, despite its status as a touchstone within U.S. culture, in part because intangible nature of privacy makes attempts at definition an exercise in subjectivity. As a result, the lack of consistent definition creates significant variance within the legal framework that serves to protect the variety of actions and interests that are defined as the privacy interests of U.S. citizens.

2. Conceptual Privacy

The malleable nature of privacy is what allows it to remain a viable concept both from a cultural and from a legal perspective. A society and its culture define privacy as the value of privacy is identified by and held within the culture that defines it (Taylor, 2011, p. 456). Privacy standards, like fashion, evolve, and what at first seems invasive and uncomfortable, can ultimately become acceptable (Baker, 2010, pp. 314–316). Given the prevalence of technology in U.S. society, and how Americans use it, what has been traditionally deemed private may no longer be assumed as such, and vice versa, as what has traditionally been deemed public may be considered private. Therefore, the effort or value attached in trying to define privacy may be questionable given the overly broad context from which privacy definitions often derive (Solove, 2006b, pp. 477–564). The rapid evolution of technology contributes to the definition of privacy, and as with technology, defining what was does not assist in identifying what exists now.

Traditional definitions of privacy are often centered on distinguishing between that which is public and that which is private, as first discussed by Plato (DeCew, 1997, p. 9). The private realm, generally equated with the home, has long been recognized within Western culture and stands for the right of freedom in association and thought (Gutwirth, 2002, p. 15). However, as with any right, society may limit the individual's exercise of privacy rights. For example, the government may be granted authority to enter

a person's home without the individual's authority through the issuance of a judicially approved warrant granting a right of entry.

Privacy is not merely an exercise in cultural definition, as it is also related to the individual's state of being. Privacy may be used as a vehicle to protect a person's relationships with others and for ensuring freedom of expression and choice (Peters, 1999, pp. 115–120). Within this context, privacy becomes an issue of self-regulation inclusive of personal associations, outward conduct, and public disclosure (pp. 115–120). This concept of privacy as a state of self-determination is supported by Westin's theory of the four states of privacy, under which privacy includes personal autonomy, emotional release, self-evaluation, and limited, controlled communications (Zoufal, 2008, p. 71). Therefore, privacy also translates to a self-identified, active role for the individual in maintaining privacy through the control of his individual's self and communications.

Technology and the use of sensors by the government to conduct mass surveillance, raises privacy concerns because it pushes the public/private boundaries. As the use of sensor technology expands, privacy in the traditional sense becomes more difficult to achieve in that the individual may not control the capture of personal images or other PII, nor retain control over dissemination of the data captured. For example, CCTV is ubiquitous in many large cities (Cameron, Kolodinski, May, & Williams, 2008, pp. 5–6). Capture of an individual's image through CCTV becomes available for many uses subsequent. A well-known example occurred in the United Kingdom when an individual was filmed during a public suicide attempt. The captured video surveillance was then later widely disseminated, both in print and broadcast, with the individual identifiable, although some versions masked his facial features, as a demonstration of the success of the U.K.'s investment in CCTV (Bickel, Brinkley, & White, pp. 357–358). While the CCTV undoubtedly contributed to saving his life, the very personal action of the individual was not subject to widespread viewing, discussion, and debate.

Within the United States, release of CCTV or LPR footage under a Freedom of Information Act (FOIA) inquiry provides individually identifying information that may be used to establish action, time, and location of individuals upon the public way, all without individual approval, and in some cases, even knowledge. Further, the

proliferation of surveillance technology may serve to chill expressive activity, as people tend to act with more restraint in engaging with other people or groups when they know they are being watched (Ozer & Schlosberg, p. 6). As control over a person's personal images and actions are increasingly removed from the individual, privacy concerns over government's mass surveillance of the public movement of its citizens will continue to grow, as will uncertainty as to how to define privacy within a digital world.

The capability for continual mass surveillance by government through use of sensor technology brings into question whether privacy can be maintained in public. While the lore of anonymity within public areas remains; increasingly, what happens in public is captured, recorded, indexed, and is retrievable far beyond the original site of occurrence (Garfinkle, 2000, ch. 5). Location, (space), is an important factor for privacy, as it is sometimes defined as a bundle of interests affected by space, but not determined by space (Taylor, 2011, p. 457). Taylor's communal view of privacy identifies four dimensions of privacy: space, time, action, and information, which are based upon context and provide the social value for secrecy, dignity, and autonomy in regards to the individual (p. 457). All four may affect privacy or only one of the communal privacy dimensions, but an individual reserves privacy in that which is not voluntarily disclosed within another social sphere (p. 457).

Mass surveillance technology attacks the communal concept of privacy in that the data not only captures an individual's travel to a location; it can be aggregated to derive a whole of information not previously accessible. For example, surveillance technology can be used to identify route of travel, frequency of travel, time, dates, type of location, and how often an individual enters a location. However, the availability of this information does not equate to a voluntary waiver of all privacy attached with the individual's use of the facility and it does not release of all privacy dimensions that attach to the individual's distinct actions for that location. Under the communal theory of privacy, certain privacy rights remain in place; for example, if the location were a medical facility, the individual

does not waive privacy as to medical conversation with the doctor, type of treatment, nature of illness, etc.[20]

The growing capacity for individuated data arising out of the government's expanded use of sensor technology to conduct mass surveillance of public movement is what brings forth concerns over the mosaic theory as discussed by the court in *Maynard* (*United States v. Maynard*, p. 562). Under the mosaic theory, which has its origination in national security intelligence, seemingly disparate items of information, although of limited value or information individually, can take on added significance when combined with other items of information (Pozen, 2005, pp. 629–630). Extrapolation of discrete data has long served to assuage the public when used for crime solving, which now generates growing privacy concerns because of mass surveillance.

The expanding role of government into the private lives of its citizens has further eroded the concept of privacy as a measure of self-determination. Control over information about an individual is a critical privacy component, as is the degree of access that others have to the information, regardless of who controls it (Nissbaum, 2010, p. 71). Privacy is also identified as the right of access, or lack thereof, to personal information (Garfinkel, 2000, p. 4). Prior to the mid-19th century, the collection of PII data by the government was generally limited to the recording of the birth, marriage, and death of individuals (National Criminal Justice Reference Service, 1977, p. 4). PII records contained limited information, and afforded minimal outside access, as they were often only available and stored locally (Solove, 2002, p. 1139). However, over time, as citizens' interaction with the government has expanded, the government generates and retains significant amounts of PII (Constance, 1995, p. 399). Both the federal and state governments develop, maintain, and access detailed PII records as a result of the various transactions between governments and its citizens (National Criminal Justice Reference Service, 1977, p. 5). As society becomes more dependent upon the data generated and

[20] Should the location be a facility for specific treatment, say alcohol rehabilitation, then the conversation may not matter much. A FOIA request could be used to identify a significant amount of information for the individual who repeatedly travels to the location. Therefore, it would beg the question as to whether a privacy right attaches.

maintained by government, technology supplies the ability to access and use PII data easily, which in turn, feeds the demand for more information.

Privacy is also defined as an expectation of limiting accessibility to a individual's personal information (Solove, 2002, p. 1140). Voluminous data, once sheltered within file cabinets of local government offices, are now readily available, often for purposes unrelated to their origination (Salzmann, 2000, p. 356). Disclosure and discussion of the status of a person's bank account may be appropriate with a tax professional, but takes on a different context if said person's subordinates in the workplace are discussing the information (Nissbaum, 1998, p. 20). Yet, the detailed PII developed by government is now an easily disseminated commodity, given the expanding capacity of technology (Solove, 2002, p. 1139).

Additionally, public policy, often through legislative action, facilitates the commodification of record information under FOIA, and a myriad of other complex state and local laws predicated upon public disclosure of government documents (Solove, 2002, p. 1139). Often, the PII contained within public documents is secondary to the document itself in regards to the FOIA production. The U.S. Supreme Court has recognized the privacy impact of FOIA requests for aggregated data. In *United States Department of Justice v. Reporters Committee for Freedom of Press,* the respondents had submitted a FOIA to the FBI for the disclosure of the rap sheets compiling the criminal records for certain individuals (*United States Department of Justice v. Reporters Committee for Freedom of Press*). The U.S. Supreme Court ruled against the FOIA request, based upon the privacy exception, and identified that the subjects had a privacy interest in the "aggregated" information, despite the individual pieces of information, the arrests, being a matter of public record (p. 764). Although the "individual events in those summaries [were] matters of public record," the Court upheld the FBI's invocation of the privacy exception to the FOIA by holding the subjects had a privacy interest in the aggregated "whole" distinct from their interest in the "bits of information" of which it was composed (p. 764). The court found that disclosure of such information would subject the individual to an unwarranted invasion of personal privacy (p. 764).

Aggregated surveillance data remains subject to FOIA absent certain exceptions. Don Zoufal, an electronic surveillance privacy expert, has noted that with LPR data, if the data does not compromise a criminal investigation, local governments may make any data retained by the system publicly available under FOIA laws (Harwood, 2010). LPR data, in turn, provides PII as to location, time, and actions of individuals to whomever inquires. Therefore, the potential for even private citizens to track the public movement of individuals using governmental surveillance technology is not inconceivable. Nor are the individual privacy interests generally considered when the government responds to FOIA—particularly if the individual targeted by the requesting party is not known or identified by the governmental agency responding to the FOIA.

Mass data collection is not restricted to the government. Private entities, including employers, banks, cellular telephone companies, and even retailers, such as grocery stores, collect significant amounts of PII (Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council, 2008, p. 121). In that information collection is a growing component of the digital economy, private sector data collection also has significant implications for personal privacy (p. 121). It has been shown that Americans are willing to disclose private information provided sufficient benefit attaches (Peters, 1999, p. 115). Often, disclosure becomes a question of relative worth—is it worth it to an individual to disclose PII to receive benefits, such as access to a social networking site, discounts on groceries, or free software?

It is a given that the knowing and voluntary disclosure of PII data is the consumer's decision right (Taylor, 2011, p. 457). However, the collection of PII data within the private sector is largely unregulated (Nissbaum, 2010, p. 45). Much of the aggregated data generated by sensor technology, and developed and retained by the data industry, are subject to disclosure without permission or knowledge of the original, disclosing party (Solove, 2002, p. 1140). If nothing else, the growth in digital data collection and dissemination of information has affected reasonable expectations of privacy, in that such disclosures have made privacy invasion more probable (Peters, 2009, p. 115). Subsequent identification of impermissible PII disclosures become

challenging, if not unlikely, as limited legal protections for privacy and PII exist. Federal statutes, such as the Privacy Act of 1974, which limits the government's use of PII, apply only to federal agencies. Other laws, such as HIPAA and The Video Privacy Protection Act, have limited privacy protections, medical information, and video rentals, respectively. However, the private sector remains largely unregulated in regards to access and use of PII.

The public/private boundaries that guide privacy determinations further break down in an era in which the social spheres of public and private life have increasing intersection. Depending upon the context under which the privacy definition is sought, privacy transmutes with the mores of the society filtering the definition (Gutwirth, 2002, pp. 20, 29). Privacy has traditionally been seen as an individual hermeneutic, which centers on freedom from excessive intrusion into an individual's life with personal control over the degree of PII disclosed (Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council, 2008, pp. 27–28). However, as technology becomes more advanced, privacy discussions become less focused on the philosophy of privacy and more upon the impact of sensor surveillance (Masiello, 2003, p. 9).

Today's world is one in which everything is linked to everything else (Barabasi, 2003, p. 7). In many urban areas of the United States, merely driving across public streets discloses potential PII through a variety of surveillance technology in use, inclusive of CCTV, LPR, and traffic cameras. Given the explosive growth of the ability to individuate data through the data mining of governmental and private databases, a growing disconnect occurs between reality and existing individual expectations of privacy and established boundaries (p. 167). As mass surveillance of public areas grows within the United States, the concept of individual decision and control over PII, and therefore privacy, becomes less of a driver for defining privacy than does society's reasonable expectations in determining what is private and what is not.

In a digital age, where voluminous amounts of information are disclosed in the execution of mundane tasks, secrecy may not be the prerequisite to privacy (*United States v. Jones*), with Justice Sotomayor concurring (p. 957). In fact, Justice Marshall in his

dissent in Smith, succinctly stated, "Privacy is not a discrete commodity, possessed absolutely or not at all" (*Smith v. Maryland*)[21] Given the growth of surveillance technology, defining privacy as a function of personal control and reserve may be misplaced given the expanding technological mashup and use of technology to conduct mass surveillance by the government. This tension, the sharing of private information for limited personal benefit versus the lack of data protection with the potential for subsequent commodification of PII data, is accelerating as the technology's capacity for sharing information grows.

3. Privacy as a Legal Concept

Various legal mechanisms, both statutory and constitutional seek to protect privacy within the United States and internationally, as a matter of comparative law. In that privacy is a compilation of a variety of interests, legal address of privacy is often specific to the interest identified (Solove, 2006b, p. 481). Within the United States, the Fourth Amendment is the primary legal vehicle for limiting the government's intrusion upon the privacy of its citizens. However, much of the constitutional-based privacy law derives from autonomy privacy, or independence in making personal decisions, with minimal subsequent focus on, or definition for information privacy, or the constitutional right to avoid the disclosure of personal information (Solove, 2006a, pp. 23–24). Given the growing impact of the information industry, this lack of definition and focus on information privacy creates a gap in Fourth Amendment doctrine and has a significant impact on real privacy.

In addition to constitutional law, state and federal laws provide a patchwork of statutory privacy protections (McCullagh, 2001, p. 133). Given the specificity of statutes, often less outcome variation exists for privacy interests protected under statute, than that seen under federal constitutional law, which is fact based. However, existing statutory protections are often limited and targeted to specific interests, such as medical privacy

[21] *Smith* stood for the validation of the third party doctrine by the U.S. Supreme Court. The release of information by the defendant in using negotiable instruments to conduct his business was found to be a voluntary release of personal information, and the government's subsequent search of those records did not implicate Fourth Amendment protections (*Smith v. Maryland*).

under HIPAA. As such, federal constitutional law remains the primary legal vehicle by which to address impermissible governmental intrusions upon the privacy of its citizens.

Comparative law provides for insight into legal privacy principles, as legal recognition of privacy is not unique to the United States. Privacy rights within many western European countries exist under both constitutional and statutory laws. Given the often shared democratic and human rights principles shared by the European Union and the United States, comparative law analysis provides for a review of the legal and policy controls in use in the European Union to help inform policy makers and legal development within the United States. However, unlike the United States, many European countries offer clearly defined privacy protections for their citizens. For example, The Netherlands' Constitution distinguishes the privacy rights of the individual and those attached to the home (The Netherlands Constitution, Article 10; Article 12. 1983). Article 8 of the European Convention of Human Rights, (ECHR), guarantees the right to private life and family life, but it also provides for restrictions of this right under certain circumstances (Morariu, 2009, p. 47). The European Union also has specific protections for PII and data privacy. The Data Retention Directive, (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006), provides for a variety of protections for the collection and transmission of PII through electronic means, which makes the provisions applicable to other European Union member states (Article 4 & Article 5). An examination of comparative law allows analysis of what statutory data protection, including data privacy with oversight of both government and private entities, and other privacy law, provides for individual privacy protections within other democratic nations.

4. Constitutional Privacy

While the U.S. Constitution does not contain a general right of privacy, one of the more controversial areas of U.S. Constitutional law in recent times has been privacy (Chemerinsky, 2006, p. 644). The U.S. Supreme Court has ruled that while the Fourth Amendment does not provide for a general constitutional right to privacy, it does provide for individual privacy protections by creating boundaries between the citizen and the state

(*Katz v. United States*, pp. 350–351). While the government's interference with the privacy of its citizens is generally governed under the Fourth Amendment, the courts have also identified limited rights of privacy within other constitutional provisions. For example, the U.S. Supreme Court has recognized that a right of personal privacy exists within the U.S. Constitution (*Roe v. Wade*). However, the Supreme Court remains steadfast in that not every governmental intrusion creates constitutional concern (*Skinner v. Railway Labor Executives' Association*). As a result, Constitutional legal doctrine on privacy is focused on the interaction between government and its citizens and what degree of governmental intrusion warrants privacy protections. The Supreme Court has recognized privacy protections for personal autonomy, identified as matters involving the most intimate and personal choices a person may make; those decisions central to personal dignity and autonomy, under the right of liberty protected by the Fourteenth Amendment (*Planned Parenthood of Se. Pennsylvania v. Casey*). While a variety of privacy interests have been recognized by the courts, the Fourth Amendment remains the primary vehicle used to define privacy interests challenged by the government's use of mass surveillance technology.

In *Griswold*, which pre-dated the *Katz* decision by two years, the Supreme Court held that while the Constitution does not explicitly provide a right to privacy, the First Amendment contains a penumbra of grants that protect individual privacy from governmental intrusion (*Griswold v. Connecticut*, p. 483). In *Griswold*, the Court was faced with a challenge to the state's right to control information and access to birth control (p. 480).[22] Finding that the right of access as a right to information that impact individual autonomy, the Supreme Court held that the state may not, consistently with the spirit of the First Amendment, contract the spectrum of available knowledge to its citizen. (p. 482). Therefore, while holding that the Constitution does not provide an express right of privacy, the Supreme Court continues to find specific, limited privacy protections to exist in various portions of the Constitution.

[22] The *Griswold* Court also held that the Court does not sit as a super-legislature to determine the wisdom, need, and propriety of laws that touch economic problems, business affairs, or social conditions, advancing its concerns about the appropriate role and process of the Court under the separation of powers doctrine (*Griswold v. Connecticut*).

A constitutional right of privacy has also been recognized within the Due Process provisions of the Constitution. The right of liberty, as granted under the Due Process Clause of the Fifth and Fourteenth Amendments, was the basis for the Court's decision in *Roe v. Wade* (Chemerinsky, 2006, p. 649). In *Roe v. Wade*, the issue before the Court as a challenge to the constitutionality of Texas' criminal abortion laws, which severely limited access to the medical procedure, except for purpose of saving the mother's life (*Roe v. Wade*). The Court, in ruling that that the Texas law was unconstitutional, held that personal rights that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty,' are constitutionally protected (p. 152). The privacy right inherent in the right to liberty under the Due Process Clause gives citizens the right to engage in private conduct without the intervention of government (*Lawrence et al. v. Texas*, p. 578). Therefore, limited privacy rights are also found within the Due Process Clause of the Fifth and Fourteenth Amendments.

The privacy impact of technology and data storage has also been of issue for the U.S. Supreme Court for many years. The Supreme Court has also distinguished between information privacy and autonomy privacy, the right of individual privacy and the right to make decisions about the individual's personal life (*Whalen v. Roe*, pp. 599–601). In 1977, the *Whalen* court identified concerns over computer-generated data and the implicit threat to privacy arising from the government's ability to aggregate the vast amounts of information available through computerized data banks and other government files (*Whalen v. Roe*). The issue in *Whalen* concerned whether the automation of previously manual prescription records and the sharing of that information for billing purposes created a constitutional privacy invasion (pp. 600–601). The Court held that the mere computerization of past practice, in this case automating prescription records, did not create any constitutional privacy violations (pp. 600–601). However, while the Court raised "the threat to privacy implicit" in computerized government files and data banks, it found that data collection by government is generally covered by a regulatory or statutory duty to avoid unwarranted disclosures and such regulations are sufficient to protect the privacy issues raised before the Court (pp. 605–607). Early court decisions on privacy

demonstrate a willingness to find constitutional privacy protections for personal conduct, and demonstrate some recognition of the privacy impact that technology generates.

While the U.S. Supreme Court continues to express concerns over the privacy impact of technology and mass data aggregation, it is no longer a hypothetical concern and daily mass surveillance continues to grow. The government's use of mass surveillance technology in U.S. society has a significant impact on privacy expectations and becomes a meme in defining privacy. As conditions change, so must the thought processes that have defined past conditions (Parfit, 1986, p. 85). The law's capacity to address the privacy impact of new technology occurs through the lens of socially accepted uses of technology and the dynamics of communication and information transmission (*City of Ontario v. Quon*, p. 2629). The Constitution, in protecting against abuses of power, must adapt to a changing world, otherwise "rights declared in words might be lost in reality" (Brandeis, & Warren, 1890, p. 194). Therefore, the privacy issues generated by the government's use of sensor technology not only affect privacy as a matter of context and cultural definition, but the omnipresence of sensor technology also affects the constitutional and legal definition of privacy, particularly as it relates to reasonable expectations of privacy as held by the individual.

B. THE TECHNOLOGY

Integral to the concept of privacy in a digital age is understanding why this is an issue that continues to vex, despite fairly well developed cultural mores on privacy. Evolving technologies present new privacy frontiers, and the intersection of privacy, law and technology is a mashup of significant consequence for civil liberties and public safety agencies. The government's use of sensor technology continues to expand as it is seen as capable of bringing greater efficiencies and strengthening evidence in criminal investigations (Wilson & Woodard, 1987, Foreword; Smith, 2011, pp. 1–2). The downside to the use of newer technology is its significant cost, unproven efficacy and reliability, and the potential for negative impact on civil liberties (Government Accounting Office, 2011; Chicago's Video Surveillance Cameras, 2011). Regardless, the privacy concerns associated with the government's use of technology can serve to inform

policy makers on how to harness technology appropriately for public safety purposes while ensuring civil liberties remain protected.

1. Sensor Technologies

New technology is continuously being developed and tested by the government, in part, based upon the belief that technology is a critical component in facilitating public safety (Evolution and Development of Police Technology, 1998). The Department of Defense (DoD) uses unmanned aircraft systems that are reliant upon sensor technologies to identify and attack targets overseas, as well as to conduct intelligence and cargo missions (Dempsey, 2010, pp. 1–4). DHS has invested in biometric technology to identify foreign visitors and to protect U.S. borders through technology, such as U-VISIT and video surveillance (Borkowski, 2011). The Transportation Security Administration (TSA) uses scanners, biometrics and explosives trace detection technology in seeking to secure air transportation (Transportation Security Administration, n.d.). Law enforcement uses the automated fingerprint identification system (AFIS), CCTV, LPR, and RFID technologies in the furtherance of public safety (Casanova & Roberts, 2012; Woodard, 1987; Perin, 2011; National Institute of Justice, 2003). However, while the specific types of surveillance technology used by the government may change overtime, the privacy concerns brought forth by new technology often remain consistent.

a. Automated Fingerprint Identification System—Old Technology, Same Issues

The privacy issues presented by the expanding network of sensor technology are similar to those faced during the introduction of AFIS in the late 1980s. Not only are fingerprints the seminal biometric identifier, but the AFIS technology is a precursor to the sensor technology of LPR and FRT. Over 30 years ago, AFIS was identified as one of the greatest technology developments in law enforcement (Wilson & Woodard, 1987, p. 1). As with many of today's sensor technologies, AFIS increased efficiencies through the use of technology and facilitated quick, efficient sharing of fingerprint data among law enforcement agencies. AFIS is the largest biometric database in the world (Federal Bureau of Investigation, n.d.). Despite the store of biometric data

that allows for rapid identification of individuals, public concern over AFIS' privacy impact is rarely raised. Little public discussion occurs around AFIS' privacy impact today, despite a growing range of verification and identification products for the government and private sector that rely upon fingerprint technology (Zoufal, 2008, p. 106).

Biometrics establish identity through PII data, which in the case of AFIS, the biometric data are the fingerprints.[23] Biometric systems do not make definitive identification, but rather probabilistic identification (NSTC, 2006, p. 8). In other words, the system makes a determination of probability of match based on the biometric characteristics supplied (p. 8). The biometric data entry into the database is unique to the individual who supplies the data, which allows for the identification and match.

AFIS also shares similar technology with LPR and FRT. For identification to occur, the database must contain the comparison data to make a positive identification —as it does not generate identification of its own (Fisher & Fisher, 2004. pp. 5–6). The identification comparison derives from an algorithm that processes the submitted data against the existing database, which for AFIS, consists of a database that includes more than 66 million sets of fingerprints (Federal Bureau of Investigation, n.d.). The true identification, e.g., the match of the individual to the fingerprint, is made through subsequent review and confirmation of the probable match produced by the AFIS algorithm (Wilson & Woodard, 1987, p. 6). Therefore, as with LPR and FRT, AFIS leverages technology to process the data for comparison in a timelier, automated process.

AFIS facilitates the identification of individuals when little other information or evidence is available (Constance, 1995, p. 401). While the ease of identification may create a level of discomfort for civil liberties advocates, technology does not create constitutional privacy issues, as merely automating a manual process does not raise Fourth Amendment protections (*Whalen v. Roe*, pp. 600–601).

[23] Fingerprints are considered individual identifiers, given the unique ridge patterns of the fingers of humans (Wilson & Woodard, 1987, p. 5).

AFIS' evolution is relevant in a review of the privacy issues generated by surveillance technology because when AFIS was first introduced, it generated legal and public policy privacy issues. For example, privacy concerns were raised about AFIS because it allowed for the identification of individuals with minimal information (Wilson & Woodard, 1987, p. 15). Other concerns were focused on gaps in the data because of existing laws and policies as to who could be fingerprinted and when (p. 15). The subsequent use and retention of AFIS data for other than criminal purposes generated additional privacy concerns, which parallel concerns present with mass surveillance technology currently in use (Constance, 1995; Goodman v. Liebovitz). Today, the use of AFIS and its biometric identification information is well entrenched within the public safety arena, as well as within the private sector for a variety of identifications uses.

The identification ability of technology and the government's use of sensor technology to conduct mass surveillance have expanded significantly since the advent of AFIS. Many of the sensor technologies in use by the government today share similar data processing capabilities with AFIS that facilitate the identification of individuals. As such, their use by the government raises analogous concerns over public policy and privacy concerns, as AFIS did initially. Therefore, as history has shown with the evolution of AFIS, current concerns over the intrusion of newer sensor technologies may be much ado about nothing. Then again, the next advance in technology may create even larger privacy concerns, given the greater capacity of many modern technologies to individuate the data collected.

b. Global Positioning Satellite

GPS has become a significant privacy issue given its prevalent use by law enforcement to conduct surveillance of criminal suspects. Unlike a tracking beeper, GPS is not merely a tracking device as it provides data over time, distance, and location (Pham, 2011, p. 3). Originally developed for military purposes, DoD maintains and controls GPS[24] (GPS.gov, 2011). The GPS system consists of three segments: the space

[24] GPS is a term specific to the U.S. navigation system. The generic term is global navigation system. For example, in Russia, the navigation system is called GLONASS, for Global Navigation Satellite System (International Committee on Global Satellite Systems, 2010).

segment, the control segment, and the user segment with the U.S. Air Force controlling the space and control segments (GPS.gov, 2011). The space component uses the one-way signals of 30 operating satellites that give the current GPS satellite position and time (Pham, 2011, p. 3). The control component consists of worldwide monitor and control stations (p. 3). In addition, the user component consists of GPS receiver equipment, which identifies the three-dimensional position and time for the location based on the signals received from the GPS satellites (ECPA Reform and the Revolution in Location Based Technologies and Services, 2010, pp. 38–39).

The government's use of GPS has capitalized upon its location identification capabilities. From a law enforcement perspective, in addition to its use for surveillance purposes, GPS has been used for a variety of purposes, from tracking law enforcement officers' locations in the field to identifying the location of callers for 911 services (Aerospace, 2005). Some states are using GPS technology to track police vehicles, including Arizona, Mississippi, and, New York (Ferraresi, 2005; McCullough, 2011; K. Moore, 2008). Some law enforcement agencies have put GPS into the portable radios carried by the officers individually (Ferraresi, 2005; McCullough, 2011; K. Moore, 2008).

GPS' ability to constantly track movement, even remotely, has proven to be a significant force multiplier for law enforcement surveillance investigations. To conduct surveillance, law enforcement officers need only to place a tracking device on the vehicle of interest, and its movement, location, and time of activity are consistently transmitted to a remote receiver (Jallad, 2010, p. 357). Given the installation of a GPS unit on a vehicle requires minimal intrusion and resources, the driver of the vehicle is often unaware of the tracking device (Shah, 2009, pp. 284–285).

Not all GPS tracking units are the same and offer varying levels of information. Some GPS units track movement in real time, while others allow remote login and access capacity to movements that may be stored on a database (Shah, 2009, pp. 284–285). Additionally, GPS technology may also be integrated with existing dispatch systems and even LPRs (pp. 284–285). As a result, while police surveillance becomes more efficient and less resource intensive using sensor technology, such as GPS,

it becomes more invasive, in that it is generally continuous and allows detailed recordation of a vehicle's movement over time, space, and distance.

GPS tracking is not limited to vehicles in that most, if not all, cellular telephones now contain GPS technology (ECPA Reform and the Revolution in Location Based Technologies and Services, 2010, pp. 7–10, 12–31). Unlike a standalone GPS tracking device, the GPS unit is carried by the individual with the cellular telephone, which allows for tracking the individual's location, including within a private home (ECPA Reform and the Revolution in Location Based Technologies and Services, 2010, p. 31). GPS data can be stored and analyzed historically, as well as be mapped through various software applications (Shah, 2009, p. 285). Further, GPS data can be linked or merged with other databases, inclusive of LPR technology (StarChase Covert Tracking System, n.d.). As a result, a more robust dataset of the individual's movement is derived. With GPS, the traditional concept of following a suspect becomes a new type of continual surveillance that comes with digital analytic tools that process current and historical data, as well as linkages with other data sets, that provides for a broader scope of surveillance than anything seen heretofore (The Constitution Project, 2011, p. 4). Further, GPS cellular telephone information is capable of tracking an individual's every movement, even that into private homes, because the telephone is carried by the individual, and, therefore, provides greater detail than possible ever before (pp. 1–2).

c. Cellular Triangulation Technology

Cellular telephone technology can derive location information independently of GPS, through triangulation location technology, known as network based location technology (ECPA Reform and the Revolution in Location Based Technologies and Services, p. 22).[25] Such technology has been used to track user location, albeit only to the area of coverage for the tower for cellular triangulation, in further aide of law enforcement investigations (Lichtblau, 2012b). Under E911 systems,

[25] Each area of cell coverage operates on a path from base station to the cellular phone, which even when not in use by an individual, sends out registration signals, usually every seven seconds, or when signal strength fails, by way of the reverse path. The registration signals contain the mobile phone's specific code identification, phone number, and home system ID (Glover, 2007, p. 1549).

emergency location features in cell phones make use of GPS either in the cellular telephone or through network based location technology to identify the location of the cellular telephone accurately (Clark, Langer, & Powell, 2010, p. 73).

The criminal investigative value of triangulation technology is significant. For example, a common practice within law enforcement known as "dumping" allows officers to receive all cellular telephone subscriber location information for any cellular phone identified as being near a location at a certain time and date (Lichtblau, 2012b). Triangulation technology has been used to track criminal and victim locations (Lichtblau, 2012b). However, dumping is not discrete, and it identifies all users in a certain location for the time and dates identified as parameters of the search. Nor is it as accurate as GPS. However, as with GPS, it raises privacy concerns in that the individual is carrying the tracking device and may be tracked without the knowledge or disclosure by the government. Regardless of whether GPS is attached by the government to a car, or if it is carried by the individual within personally owned technology, Fourth Amendment determinations that continue to be based upon the use and type of technology, *the how*, rather than the privacy issues of those subject to surveillance, *the what*, constitutional law will continue to fall short of the needed guidance for both government and civil libertarians.

d. Automated License Plate Readers

LPR is a relatively new technology that generates tension between the competing interests of government efficiency and individual privacy. LPR technology arose out of the UK's desire to better track and identify vehicles within the United Kingdom given the government's concerns over terrorism in the early 1980s (Perin, 2011, p. 1). Within the United States, LPR is used for routine law enforcement surveillance by various agencies, including the Chicago Police Department, the Los Angeles Police Department, the Virginia State Police, and a host of other law enforcement agencies (IACP, 2009, pp. 1–3). While LPR use is newer to the United States, it is being assimilated rapidly. For example, within Chicago, LPR is not only used by law enforcement, but it is also used for issuing parking violations for street

sweeping.[26] Syracuse, New York is mounting cameras to school buses to capture traffic violations, e.g., cars passing the school bus when stopped (Mason, 2008). Some governmental entities also use LPR for administrative purposes, such as parking tickets (Manson, 2008). While LPR technology shares similar structure and components, the policies that control when and how data is collected and stored create variance in LPR data and the resulting privacy impact.

LPRs are a form of video surveillance with a targeted function, to identify license plate information (Obeid et al., 2007, p. 486). All LPR systems share the same basic technology structure, with the overall quality of the images affected by the quality of the component parts (p. 486). LPR uses video camera images to identify license plate character information (p. 486). LPR cameras can be fixed or mobile (IACP, 2009, p. 21). Fixed post cameras are generally based upon traffic flow or some other determinant, and portable cameras are generally mounted on police vehicles (p. 21). However, portable LPR is also being deployed as a means to allow fluid response to identified needs and to limit the drain on law enforcement officers from the field needed to monitor and await response from the LPR data hits (Prototype Portable LPR System Provides Options, 2012, p. 1). Portable LPRs are generally mounted to a moving platform that can remain as a standalone LPR but be moved as needed, such as a trailer (p. 1).

LPRs have five general components: 1) a sensor that provides intake for the data and reduces it to a standardized template and data storage format, 2) the processing algorithm that takes the input data and formats it for analysis, 3) the data storage, 4) the analytic algorithm that processes the data against the outside, or match data, and 5) the determination of probability (NSTC, 2006, pp. 3–5). As seen with other sensor technology, the actual match, e.g., confirmation of identity, occurs through subsequent review of the probable identification, either through human review or through technology (pp. 3–5).

[26] The LPR camera system is mounted on the street sweeper, which then photographs the license plate number and a picture of the vehicle that was not removed, as required under City ordinance, from the street during street sweeping days. A parking violation notice is then mailed to the identified to the registered owner of the vehicle, information that is not kept within the LPR system itself (Manson, 2008).

LPRs use a recording device, usually a high-speed camera, which then feeds data to the algorithm that converts the license plate data so it can be read against the supporting database (IACP, 2009, p. 5). Once the image is captured, the system utilizes character recognition to define the license numbers for the consistent reading of the data (Obeid et al., 2007, p. 486). Both sets of information, the image, and the subsequent comparison within the database, are achieved through the use of algorithms to extract and identify the data (p. 486).[27]

The accuracy within LPR systems is dependent upon the quality of the captured image for the validation of the license plate information (IACP, 2009, p. 5). Various factors, from lighting to environmental conditions, affect image quality, which is why LPR cameras generally use both regular and infrared camera images to enhance data collection (p. 5). Many LPR systems are also linked with GPS that allows capture of the time and location information in addition to the license plate information (p. 6). Linkage to other databases and systems extends the depth and breadth of the LPR monitoring capacity rather than just capture of a license plate image.

Assuming accuracy within the underlying technology, the identification probability of a LPR image is only as good as the data within the comparison system (NSTC, 2006, p. 11). LPR data is run against a comparison database, which generally contains license plate information, the comparison data. Most agencies utilize the National Crime Information Center (NCIC) databases, which are maintained by the Department of Justice (National Crime Information Center).[28] Local law enforcement

[27] Algorithms, generally proprietary, perform optical character recognition using six consistent functions to identify a license plate including:

1. Plate localization, which finds and isolates the plate contained in the picture;
2. Plate orientation and sizing, which compensates for the skew of the plate and adjusts the dimensions to the appropriate size and shape;
3. Normalization, which adjusts the brightness and contrast of the image;
4. Character segmentation, which finds the individual characters on the plates;
5. Optical character recognition, which converts the image into actual characters; and
6. Syntactical/Geometrical analysis, which checks characters and positions against state based law or internal agency policy to identify the state issuing the license plate (IACP, 2009, pp. 5–6).

[28] NCIC is a national database of criminal justice information available only to law enforcement, and includes information, such as criminal record history information, arrest warrants, and stolen vehicle information (NSTC, 2006, p. 11).

agencies usually maintain a separate, local database, where they can add additional information, pursuant to the policies established by the agency that owns the LPR system (Perin, 2011, p. 2). For example, local databases may also include local warrants associated with the owners of the license plates, the validity of the driver's license for the owner of the license plate, or other priorities as identified by the entering agency (p. 2).

LPR systems allow for easy access to information already in the public realm and aggregates it for analysis and dissemination (IACP, 2009, p. 12). While the LPR system does not contain PII, it associates the LPR data with other databases that then can provide the ability to individuate the information and obtain PII (pp. 9–10). The more linkages of PII to license plate information, the more individuated the data becomes, and thereby, increases privacy concerns. Further, LPR's ability to access and link to information and its significant storage capabilities are of growing concern to some civil libertarians given the lack of consistent policies for database retention and sharing (Johnson, 2011).

In that as a matter of function LPR requires linkage with other databases to make probable identifications, it creates privacy concerns. The initial LPR data captures the license plate image, and has no intrinsic value; rather, it needs to be linked to another data source, such as plate registration information to derive investigative value. For example, within the United Kingdom, license plate reader technology, called Automatic Number Plate Recognition (ANPR), has been integrated into larger databases including the target hardening and the security plan known as the "ring of steel" within London (Coaffe, 2004, pp. 204–209). All the ANPR data for England, Scotland, and Wales is stored within one centralized computer database (Bilton, 2009). Not only does the United Kingdom have a large, aggregated database for vehicle identification, it also inputs all criminal offenders wanted anywhere within the United Kingdom (Bilton, 2009).

LPR is designed for database extraction and sharing; thus, its aggregation capacity is inherent within the technology design. However, LPR technology can be used to preserve, or least enhance, privacy. Some LPR technology has the ability to blur the facial and license plate images captured by LPR automatically through pixilation (Malin,

Newton, & Sweeney, 2003). However, at this time, no simple way exists to classify the features of an image into automated data rules for general masking techniques (p. 21).

Even with masking technology, comparison between shared databases can still occur through the underlying data while limiting the government's intrusion into the privacy of the individuals under surveillance.

Even absent technology, LPR systems can be programmed to limit privacy concerns through codified retention and use policies. For example, during the tour of duty, the South Portland, ME police department allows vehicle license plates to be entered by officers for a variety of reasons, but purges these entries at the end of their shift (Perin, 2011, p. 2). In addition to purge programming, policy can serve to limit retention and individual privacy impact, even if technology cannot do it independent of human intervention. Given the HLS field's interest and appetite for data analysis within multiple databases, data mining through LPRs becomes a growing area of concern for privacy advocates (Strandburg, 2008, p. 476).

e. Radio Frequency Identification

RFID is a form of sensor technology known as automatic identification and data capture (AIDC) technology that uses electric or magnetic fields at programmed radio frequencies to transmit information associated with a tag (Barber, Bunn, Eydt, Karygiann, & Phillips, 2007, p. ES-1). Other auto-id systems include technologies, such as barcodes, smart cards, and optical character recognition systems (Brito, 2004, p. 2). RFID has a variety of uses, including asset management, inventory tracking, security access control; digital payments, and even for personal identification (Barber et al., 2007, pp. 3-1—3-6).

A RFID system has two main components, the RFID tag and the RFID reader (Anagnostopoulos, Anagnostopoulos, Giannoulos, Kayafas, Kolias, & Loumos, 2010, p. 2). The tag contains a digital number associated with the physical object to which it is attached (p. 2). The reader is generally connected to a backend database and operates as a radio transceiver that communicates with the transponder or tag via radio

waves (Brito, 2004, p. 4). RFID tags are always “listening” for radio signals sent by RFID readers, and when the appropriate query is received, the tag responds by transmitting the unique ID code stored in its memory back to the reader (p. 4). While RFID technology is similar to barcode technology in that it provides tracking for specified objects, it also provides greater information value because it can read the tag outside the line of sight, has greater data capacity, enhanced reading distance, and the ability to link tag information to a variety of databases (Barber et al., 2007, p. 2–1). RFID technology reduces the need for human involvement in the identification process and can record historical information regarding the movement or location of the tagged item (p. 2–1). RFID is a strong technology for deriving location information, provided the system is maximized for read capacity, signal strength, and time of scanning (Anagnostopoulos et al., 2010, p. 2).

RFID tags are either passive or active. Active tags have an independent power source and transmit signals autonomously over distance and time (Barber et al., 2007, p. 2–5). Passive tags are cheaper and last longer, but require an external source for power and to transmit and record a signal (p. 2–5). Unlike other signal-based tracking systems, such as Wi-Fi tags or Bluetooth, RFID is relatively low cost (Anagnostopoulos et al., 2010, p. 3). The tradeoff for a simple, (cheaper), RFID system is that RFID tags can be cloned easily, absent cryptographic security measures, which may lead to economic and information loss (Seuschek 2010). Further, RFID shares similar signal degradation problems with other signal-based technology systems, including environmental interference, suitability of the location being tracked, and the need for proximity of the reader based on the system used (Anagnostopoulos et al., 2010, p. 3). Growing concern is increasing over the use, type, and security of RFID systems as they relate to individual privacy impact (Electronic Privacy Information Center (EPIC), n.d.d.).

The government uses RFID for a variety of purposes, including facilitating the management of the supply chain for emergencies and large-scale disasters (Seuschek, 2010). The U.S. military uses RFID technology for inventory control, and tracking a range of items from uniforms to armored tanks (Brito, 2004, p. 13). RFID is growing in

use for toll collections and is used in states, such as Illinois, Virginia, Pennsylvania, and Maryland.[29] Under the E-ZPass system, LPRs are mounted at the toll collection sites, to capture both front and rear license plate information (E-ZPass Group, n.d.). Users place the RFID-enabled toll transponder in the window of their vehicle that is subsequently read at the collection point and the retrieved information is fed into the appropriate database that deducts the toll from the user's account by cross-referencing the license plate to the appropriate toll account (E-ZPass Group, n.d.).

Document tracking is another possible use of RFID within the HLS field, as demonstrated by the Real ID (Electronic Privacy Information Center, 2008). The Real ID is essentially a plan for a national identification card and is seen as a means to enhance national security, guard against terrorists and illegal immigration (Electronic Privacy Information Center, 2008). Privacy advocates raise concerns to the contrary citing the lack of demonstrated need, historical aversion to national identification, and the PII creep of social security numbers (Electronic Privacy Information Center, 2008). While the National Real ID act remains subject to ongoing political debate,[30] under the Western Hemisphere Initiative, (WHTI), the DHS has installed RFID readers at the top customs entry points to the United States to enable quicker entry processing of travelers to the United States (Napolitano, 2009). The majority of U.S. and Canadian citizens were already using WHTI-compliant documents at border crossings and over 950,000 RFID enabled passport cards have been distributed by the Department of State as of 2009 (Napolitano, 2009). Despite privacy concerns, the use of RFID documents is growing.

Several states are also using RFID technology in identification documents, including EDLs. These states include New York, Vermont, and Washington (Homeland Security, n.d.b.). The EDLs are imbedded with an RFID tag that signals a secure system

[29] See http://www.ezpass.com/static/links/index.shtml for a listing of states using RFID technology under EZPass.

[30] Congress passed the REAL ID Act as part of the Emergency Supplemental Appropriations for Defense, the Global War on Terror and Tsunami Relief Act (P.L. 109-13) and it was signed into law by President Bush on May 11, 2005 and effective January 15, 2013. "The REAL ID Act established minimum standards for state-issued driver's licenses and identity documents that are used for Federal purposes, such as to enter a Federal building or a nuclear power plant or to board an airplane." (Secure Identification, 2012). Controversy continues over the implementation of the Real ID Act and what implementation means relative to privacy (Secure Identification, 2012; EPIC, n.d.b.).

to identify the biographic and biometric data associated with the person issued the EDL (Homeland Security, n.d.b.). A Machine Readable Zone, (MRZ), which is basically a scanner, allows the CBP officer to read EDL bar code information if the EDL is presented at a crossing not equipped with RFID (Napolitano, 2009).

RFID's use within the HLS arena has been primarily for asset tracking and identification documents. Yet, the key strength that RFID provides is the ability to identify real time location, which facilitates mass surveillance (Anagnostopoulos et al., 2010, p. 2). Given its ability to provide unique identification, based upon the tag, RFID continues to be of interest not only for its identification abilities, but also for its ease of integration with other surveillance technology, including CCTV (pp. 4–5). As a result, RFID raises considerable privacy implications given the relative ease in which RFID signals can be read and/or intercepted. Given the expanding use of RFID in PII documents, such as EDLs, data protections for RFID are as important as the data efficiencies created by technology.

2. Aggregation Capacity

The immediate privacy interests raised by surveillance technologies, the initial intrusion, have been the center of most discussions around their growing prevalence within U.S. society. However, concerns over the back end, the creation of mega databases and network analysis techniques or other data mining, are growing (Strandburg, 2008, p. 795). The government's ability to engage in continual mass monitoring of the daily lives of individuals, combined with the increased detailed information these systems generate, stands to create new opportunities for combining data elements to generate greater amounts of and access to PII (Barber et al., 2007, pp. 6–3). Through various technological developments, the use of one sensor technology can link to and data mine other technologies to create more complete information.

In a world in which mass surveillance is common, economies of scope are driving data aggregation, as seen with the mega databases resulting from AFIS and the ANPR national database in the United Kingdom. Moreover, not just the government is looking to further aggregate PII data. Commercial development is also seeking to harvest the full

value of the information rich society in which everyone lives. For example, the Mobile Offender Recognition and Information System (MORIS), can identify a person via FRT or through iris scanning (Seifert, 2011).[31] MORIS can operate from a common smart phone's camera to obtain the subject's picture and to take an iris scan, which is then run through a backend database to develop an identification match probability (Seifert, 2011). MORIS also uses biometric identification through fingerprints that are also obtained through use of the smart phone (Seifert, 2011). As with any sensor technology, access to the comparative data is required to ensure appropriate identification probabilities. In the case of MORIS, general commercial viability is possible provided access to a supporting database is available, such as facial photograph images for FRT and fingerprint data.

Another example of growing commercial development is the use of validity sensors[32] on mobile devices. A mobile device or tablet screen can be equipped with fingerprint recognition technology that functions within the device, with minimal interference with operations, and thereby, creating greater security than a traditional password (Planet Biometrics, 2013). Despite not yet having any customers for this sort of technology, Apple is seen as positioning itself to incorporate such technology within its iPhones (Planet Biometrics, 2103).

Facebook's "tag" program is another example of the commercial development of sensor technology. FRT housed on Facebook's servers scans users' uploaded photographs of individuals for possible matches, which once confirmed, allows users to "tag" a large set of photos quickly (Paul, 2011). This technology also allows for rapid identification of other associations within the Facebook system, independent of the user uploading the image (Paul, 2011). The popular line "there's an app for that,"[33] might well apply to the commercial use of a sensor system for the smart phone. The technology continues to expand, thereby creating a growing data economy not controlled by the

[31] The MORIS manufacturer is seeking approval from Apple, Inc. to allow application permission, "app," from Apple, Incorporated to allow function on the I-phone platform (Seifert, 2011).

[32] Validity sensors are nearly invisible and provide enterprise-grade security by verifying the fingerprint used on a button or pad and sent to the host processor with the one matched on-chip (Highest Performing Fingerprints Sensors for Handsets, Tablets and PCs, n.d.).

[33] Apple, Inc. has received trademark rights to the slogan (Chen, 2010).

government nor fully regulated as a private enterprise and individuals are not subject to most existing privacy laws.

The mega data that results from mass surveillance creates a conduit for access to PII by both government and private entities. One example is the automated toll readers that allow for mass surveillance of travel and location of vehicles upon the toll ways and, presumably, their owners or drivers. The New York Department of Transportation tracks vehicles in real time, through linkage to E-ZPass that uses RFID technology (NYSDOT, 2007). The availability of such data results in requests for surveillance camera, LPR, and toll way reader data, and has become a matter of regular practice for legal discovery to either prove or disprove travel and presence across the toll ways (Newmarker, 2007).

Some toll way authorities, cognizant of the privacy implications of automated toll collections, offer anonymizing practices, such as the ability to purchase a pre-loaded pass for a certain amount without disclosing PII data (TxTag, 2011; Landis, 2009). Other states have relied upon legislation to protect the PII of tollway users with RFID toll passes. For example, the State of Illinois limits access to, and therefore, the privacy impact of PII data derived from electronic toll collections systems. The PII deriving from toll collection systems may not be sold or provided to any person (605 ILCS 10/19.1(b)). PII is broadly defined as any information that describes a user, including information that identifies travel pattern data, address, telephone, email address, license plate number, photograph, bank account information, or credit card number (605 ILCS 10/19.1(a)). Further, under 605 ILCS 10/19.1(g), PII generated through electronic toll collection system is exempt from FOIA. Therefore, privacy concerns generated through sensor technology are addressable through technology and legislative action.

The ability of sensor technology to capture and store information also brings forth significant back-end privacy issues around data sharing and data aggregation. The depth and breadth of detailed PII available through sensor technology, that is then subject to unlimited retention and data mining, stands to alter the relationship between the government and its citizens (*United States v. Jones*), with Justice Sotomayor concurring (p. 956). The privacy concerns generated by sensor technologies, such as RFID and LPR, are interrelated with security considerations and system development address both

privacy and security during development (Barber et al., 2007, pp. 6–3, 6–14). Today's technology increasingly blurs the distinctions surrounding the government's proper use of technology given the mass surveillance, aggregation capacity, and connectivity of databases (Zoufal, 2008, p. 113). Further, while minimal statutory regulation exists for PII data within the government sector, little to no oversight occurs within the private sector data information business (Woodard, 1998, p. 7). Despite voicing its concerns over data aggregation for decades, the U.S. Supreme Court and Congress have done little to ensure the privacy of U.S. citizens in a digital age.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. LEGAL ANALYSIS OF U.S. PRIVACY LAWS

The Fourth Amendment serves to define the limitations on the government's use of sensor technology to conduct surveillance of the public movements of its citizens. The protections of the Fourth Amendment are not stagnant, but rather derived from evolving social norms, practices, and expectations (Marceau, 2011, p. 705). However, establishing the legal boundaries for law enforcement's permissible use of surveillance technology has been an arduous and circuitous process as evidenced by the progression of technology-related privacy decisions of the U.S. Supreme Court.

A. FOURTH AMENDMENT ANALYSIS

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…
>
> U.S. Constitution, Amendment IV

Absent a search, no Fourth Amendment privacy issue exists. Surprisingly, defining "search" under the Fourth Amendment remains elusive and it is not readily defined within existing case law (Hutchins, 2007, p. 422). Generally, a search exists for Fourth Amendment purposes when the government takes an action that infringes upon an individual's assertion of privacy over said individual's self, home, papers, and/or effects and (1) has demonstrated a subjective expectation of privacy, and (2) society is willing to recognize the expectation of privacy as objectively reasonable (Kerrane, 2011, pp. 1705–1706). The Supreme Court has interpreted the Fourth Amendment in an erratic and occasionally contradictory manner (Hutchins, 2007, p. 422). As a result, Fourth Amendment doctrine lacks consistent guidance for law enforcement in determining the appropriate standards for the use of technology to conduct surveillance.

In the digital world in which Americans work, play, and store their personal effects, the U.S. Supreme Court struggles to marry the underlying Fourth Amendment concept of "place" with the virtual world in which Americans increasingly spend their time. In 1967, the Supreme Court held that the Fourth Amendment protects people rather than places (Katz v. United States, p. 351). However, this pronouncement belies the

history and continuing focus of the Court's Fourth Amendment analysis. In its 2012 decision in the *Jones* case, the U.S. Supreme Court stated: "the text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to "the right of the people to be secure against unreasonable searches and seizures"; the phrase "in their persons, houses, papers, and effects" would have been superfluous" (*United States v. Jones*, p. 945). The U.S. Supreme Court continues to tether privacy to a concept of place. Courts appear to deal better with resolving privacy issues if they track traditional concepts of privacy, such as physical intrusion (Solove, 2006b, p. 564). However, as technology reduces the need for "place" to store personal affects and a reduced need for physical, or even cognizable, intrusion by government to delve into the private realm of citizens occurs, the traditional boundaries of constitutional limitations on government surveillance begin to blur.

As stated, the Supreme Court decisions on privacy and technology vary and lack consistency. On the one hand, the Court has held no constitutional Fourth Amendment protection exists for what a person knowingly exposes to the public, even within the home (*Lewis v. United States*).[34] Yet, the Court has also recognized that Fourth Amendment constitutional protections may apply if someone seeks to maintain a private reserve, even if they are in public (*Katz v. United States*, p. 352). The Court has also stated that no constitutionally protected zones of privacy exist (pp. 351–352). However, in *Kyllo*, the Court carved out specific privacy protections for the home by identifying that all details are intimate details within the home, because the entire area is held safe from prying government eyes (*Kyllo v. United States*, p. 37).

The Fourth Amendment doctrine of *Katz*, which is fact drives and requires courts to analyze an individual's subjective assertion of privacy, coupled with the courts' perceptions of social expectations of reasonableness, contributes to the lack of consistency in privacy law. In part, the failure to provide sufficient definition to privacy

[34] In *Lewis*, an undercover government agent entered the home of a narcotics seller to purchase narcotics after being invited in to do so. The defendant argued in that he was a government agent, a warrant was needed. The Court held that the home was a location chosen by the defendant and within the parameters of the facts before the Court, the government's conduct did not constitute a constitutional violation (*Lewis v. United States*).

occurs because courts have a tendency to shortcut the *Katz* analysis due to a lack of empirical data to identify "society's" reasonable expectations of privacy when technology is involved (Freiwald, 2007, pp. 8–9). Further, as the government's use of surveillance technology expands, determining the evolving boundaries of private space starts to fall apart in a world in which the physical location of information is of dwindling importance (Wells, 2009, p. 223). What places and what actions are afforded constitutional privacy protections will change as privacy intrusions become increasingly digital and the measure of governmental intrusion, within the physical sense, becomes a relative term. As such, the growing use of mass surveillance will continue to exploit the gaps within Fourth Amendment doctrine.

B. CONSTITUTIONAL PRIVACY LAW AND TECHNOLOGY—HOW DID WE GET HERE?

In regards to the confluence of technology and privacy, the Fourth Amendment doctrine and its implications for mass surveillance by government continues to evolve. U.S. law is precedential, which means that earlier decisions drive subsequent judicial analysis and determination. Unfortunately, legal privacy determinations based upon case law deriving from older technology may fail to account for the greater intrusiveness of current technology or recognize key distinctions in its use or application (Hutchins, 2010, p. 1187). Privacy decisions about the use of public phone booths have little practical translation in a world in which conversations in public move with the individual. As a result, the existing legal guidance is less than clear for law enforcement's use of sensor technology under the Fourth Amendment. However, an understanding and review of the precedent informing current law on mass surveillance and technology provides a foundation for key issues driving the decisions of the courts and clarifies how the law got to where it is at this time.

1. Olmsted v. United States

The Supreme Court's 1928 decision in *Olmstead v. U.S.* held that the purpose of the Fourth Amendment was to protect against the use of governmental force to search or seize a man's house, person or effects and to prevent their seizure absent permission

(*Olmstead v. United States*). At issue before the court was whether the government engaged in a search when it electronically tapped eight telephones over a period of nearly five months (p. 471). The government attached a listening device outside the home to listen over telephone wires to conversations occurring inside the home (pp. 456–457). The *Olmstead* court held that for the Fourth Amendment to be implicated, the government has to have engaged in a physical search and seizure of a person, material effects, or an actual physical invasion of the home (p. 466). The Court found that the Fourth Amendment did not prevent the government's use of the "senses" in listening to the conversations and noted that all surveillance actions occurred outside the home without any entry into the home or a seizure of things (p. 464).

Justice Brandeis dissented[35] noting that "rights declared in words might be lost in reality," and strict adherence to protecting things under the Fourth Amendment ignores the more subtle and far-reaching means available to the government to invade privacy (*Olmstead v. United States*, p. 474). Brandeis argued the Constitution granted not just mere protection of property but the right to be left alone, one of the most prized rights of civilized men (p. 474). Brandeis argued that to protect Constitutional privacy rights, unjustifiable government intrusion upon the privacy of the individual, regardless of whether it constitutes a physical intrusion, must be held a violation of the Fourth Amendment (pp. 478–479).

Justice Brandeis' dissent frames one of the core privacy issues that exists today relative to the use of technology by the government to conduct mass surveillance. Should governmental intrusion into the private realm be measured by the technical—the level of intrusion; or, by the conceptual—the right to be left alone, in determining whether constitutional protections are warranted? Over time, privacy theory and the decision of the U.S. Supreme Court have evolved *Olmstead.* The Supreme Court retreated from the

[35] Within the U.S. Supreme Court, a majority opinion establishes a binding precedent pursuant to *stare decisis.* However, Supreme Court justices write additional opinions to the majority decision that either concur or dissent with the decision of the majority. While not binding law, they provide insight as to the inner workings and decision matrix of the court. However, some argument is raised that plurality opinions and even concurring might contribute to precedential law as well, which serves only to add to the point of this thesis that case law is not the ideal way to define privacy in a digital world (Ledebur, 2009).

Olmstead's bright line division between home and public in providing Fourth Amendment protections beginning in 1967 with *Katz v. United States*.

2. Katz v. United States

In *Katz v. United States*, the Supreme Court provided privacy protections for intangibles under the search and seizure limitations against the government under the Fourth Amendment (Maceau, 2011, p. 687). At issue in *Katz* was whether the conversation of an individual inside an enclosed public telephone booth was entitled to constitutional protection from government surveillance under the Fourth Amendment (Katz v. United States). The *Katz* court stated that the failure to provide privacy protections to individuals within the public arena ignores the critical role of evolving technology (*Katz v. United States*, p. 353). In finding that the government's action was a search under the Fourth Amendment, the *Katz* court held that the Fourth Amendment protects people, not just places (p. 352).

Despite overruling the property-based focus of *Olmstead* and expanding Fourth Amendment protections beyond the home, the *Katz* court refused to find that the Constitution granted a general right to privacy (*Katz v. United States*, p. 351). Significantly, the *Katz* Court held that Fourth Amendment privacy protections were predicated upon whether the individual had a subjective expectation of privacy and whether society was willing to recognize that expectation as reasonable (pp. 352–352). While *Katz* is predicated upon a subjective exercise of control as a means of demonstrating an expectation of privacy, the reasonable expectation of privacy is identified, and defined, by the trier of fact, and not the individual making the claim of a privacy right (Rubenfeld, 2008, pp. 106–107). In effect, the Court expanded upon the *Olmstead* determination of constitutional privacy protections for property by substituting terms people for places and privacy for property (Clancy, 2012, pp. 306–307).

Justice Black dissented, arguing that the Court improperly expanded the Fourth Amendment to cover general privacy rather than establishing a limitation on the government's authority under which it could conduct searches and seizures of its citizens

(Clancy, 2012, p. 373).[36] In what he characterized as abandoning the Fourth Amendment standard of governmental intrusion to find constitutional standard to include a more generalized privacy right, Justice Black argued that the Court was expanding its powers into an ongoing constitutional convention (p. 373). Such decisions, according to Justice Black, were better addressed through Congressional legislative action given the constitutionally mandated separation of powers (p. 373).

In a rapidly expanding virtual world, Fourth Amendment privacy expectations and the social norms that define reasonable expectations of privacy remain unsettled. Although the *Katz* standard is one of reasonableness, it does, in part, re-emphasize the concept of the individual's relation to the claim of privacy (Clancy, 2012, pp. 306–308). As noted by Justice Harlan, determinations of privacy generally do not occur without reference to a place, despite the assertion that the Fourth Amendment protects people (*Katz v. United States*, p. 361). The focus on place under Fourth Amendment doctrine has challenges in defining privacy when technology requires limited or no physical intrusion to access, which serves to confuse the subsequent constitutional analysis (Wells, 2009, pp. 229–230). Given the growth in surveillance technology and capacity, a timely and coherent precedential legal framework for decision is needed if the Fourth Amendment is to remain a viable vehicle for the protection of individuals against increasingly intrusive action by government (Marceau, 2011, p. 699).

Mass surveillance technology alters the individual's control over personal data and actions upon the public way. The *Katz* doctrine, with its circular standard of reasonable expectations of privacy, skirts a key privacy issue for today's state of mass surveillance—does the prevalence of observation and even surveillance in U.S. society negate a reasonable expectation of privacy in public? In a modern society in which the pervasive presence of sensor technology has people accustomed to continual surveillance, diminution of constitutional privacy protections, based upon the *Katz* reasonable

[36] Justice Alito finds problem with the seemingly inapposite position of the Court in the 2012 decision in *Jones v. United States.* He argues the majority decision in *Jones* contravenes *Katz,* in that the Court wrongly relies upon a finding of technical trespass by the government is sufficient to find that a search occurred for Fourth Amendment purposes rather than deciding on reasonable expectations of privacy (*United States v. Jones*, pp. 959–961), with Justice Alito concurring.

expectation of privacy analysis, is not without concern (Hutchins, 2010, p. 1193). Given mass surveillance, the problem for privacy is can an individual claim a reasonable expectation of privacy on the public way, given the proliferance of surveillance technology in use by the government and privacy entities? Therefore, hypothetically at least, the government could overcome subjective and objective privacy expectations by posting notice not to expect any privacy in regards to sensor surveillance (Chemerinsky, 2006, p. 650). Whether the prevalence of mass surveillance serves to negate any reasonable expectations of privacy in public, as defined under *Katz,* has yet to be addressed by the U.S. Supreme Court.

3. Third Party Doctrine

Third party doctrine has significant impact on privacy decisions where technology is part of the fact pattern. Under the third party doctrine, the courts have held that the government can use information disclosed by an individual to a third party without implicating Fourth Amendment protections. In *United States v. Miller*, at issue was whether the government's access to an individual's bank records was an impermissible search under the Fourth Amendment (*United States v. Miller*). The respondent argued he had a Fourth Amendment interest in the records kept by the banks because he had a reasonable expectation of privacy in that they were copies of his personal records and were made available to the banks for a limited purpose (p. 442). However, the U.S. Supreme Court ruled that the individual assumes the risk that when revealing affairs to another, that the information will be conveyed to the government by that person (p. 443). Further, the Court held that banking records were not confidential communications, but, rather, negotiable instruments voluntarily exposed to third parties, which did not provide for a reasonable expectation of privacy (pp. 441–443). Even if the individual held an expectation of privacy based on an assumption of confidentiality, the Court ruled that society was not prepared to recognize such an expectation as reasonable (pp. 441–443).

Therefore, does the use of technology vitiate a reasonable expectation of privacy? With the advent of the web and cloud computing, many personal transactions and much private information is generated and stored in a third party environment. Exposure of

information to a third party is a given where most digital data is remotely stored or accessed (Wells, 2009, p. 230). The U.S. Supreme Court has not decided a third party doctrine case in the modern era in which social norms and technologies dictate that vastly more PII resides with third parties, as a matter of routine business requirements (Henderson, 2011, p. 42). As noted by Justice Sotomayor, the third party doctrine is ill-suited to the digital age where people necessarily disclose significant amounts of personal data just engaging in daily business (*United States v. Jones*, p. 957), with Justice Sotomayor concurring. Even the U.S. Supreme Court has pondered whether new technology entails a trade-off between convenience and privacy, with the issue being whether technology inevitably reduces privacy as a matter of law (p. 962). The existing Fourth Amendment doctrine defines privacy interests within a framework based upon governmental intrusion, rather than privacy principles.

Cellular telephones provide context for the insufficiency of Fourth Amendment privacy protections. By merely possessing a cell phone, which has become ubiquitous in today's society, it is possible to surrender location privacy. Tracking technology that uses cell tower information to locate a cellular telephone is not considered a Fourth Amendment search, under the theory that the cell phone signals are knowingly exposed to a third-party—the cell phone company (*United States v. Bermudez*). In *Bermudez*, the government used an electronic device and cellular telephone tracking technology to identify the location of purported narcotics activity, including the residence of the targeted individual (*United States v. Bermudez*). The *Bermudez* court ruled pursuant to 18 U.S.C. § 2701 *et seq.* (the Stored Communications Act) and 18 U.S.C. § 3121 *et seq.* (the Pen/Trap Act) and under Fourth Amendment review that the government acted within the law in capturing the electronic signals of the telephone that emanated from inside the house, given that no reasonable expectation of privacy was anticipated in the transmission of the cellular telephone signals (*United States v. Bermudez*). The court relied upon third party doctrine citing that the owner knowingly transmitted signals to the third party, and if a desire existed not to do so, all that had to be done was to turn the cellular telephone off (*United States v. Bermudez*).

As recently as 2012, the 7th Circuit reaffirms that no reasonable expectation of privacy exists concerning cellular telephone numbers, and perhaps even for information contained therein (*United States v. Flores-Lopez*). At issue in *Flores-Lopez* was whether a search for Fourth Amendment purposes occurred when the government looked at the cellular telephone to obtain information without a warrant (p. 805). The court likened the access to the phone as similar to obtaining information from a diary discovered upon the person arrested, which is permissible under the Fourth Amendment (pp. 806–807). The court further held that obtaining the cellular number information from the phone was also permissible, because by subscribing to the telephone service, the user of the phone is deemed to surrender any privacy interest this user may have had in the phone number (p. 807).

In 2011, law enforcement made over 1.3 million requests for cell subscriber data from cellular telephone companies (Lichtblau, 2012a). Additionally, law enforcement is increasing its use of cell tower location services. AT&T reported a triple increase in law enforcement requests as compared to 2007 (Lichtblau, 2012a). However, as noted by the *Bermudez* court, law enforcement's use of real time cell site information for surveillance is a relatively new tool and Congress has yet to provide specific legislative boundaries on the practice (*United States v. Bermudez*). As a result, under third party doctrine, possession of a cellular telephone may properly act as a tracking device for the government without the knowledge or permission of the individual carrying it. While this is the decision of the 7th Circuit Court of Appeals, the analysis could apply to any court absent legislative control of the issue.

While not on point, the U.S. Supreme Court has reviewed the individual right of privacy in the use of a texting pager provided by the government to an individual (*City of Ontario v. Quon*). In essence, the employee had used the text pager to send messages he considered private; however, the government employer accessed those messages and took a job action as a result (p. 2622). When the Court evaluated the invasiveness of the government employer's action, it stated that the audit of the employer provided pager was "not nearly as intrusive as a search of his personal e-mail account or a wiretap on his home phone line" (p. 2631). Missing from the Court's discussion was any mention of a

cellular phone, despite its recognition of cellular telephones as pervasive in today's society (p. 2631). Therefore, while the Court specifically recognized a lesser protection in pager text messages as compared to a personal email, it completely sidestepped whether the lesser protection for text messages to a pager would also extend to cellular telephones, one of the more robust texting modalities in society. The exponential increase in data mining of the location of individual cellular telephone owners may be a tradeoff for the convenience of owning a cellular phone, but the current law comes as a result of the Court's failure to provide guidance or even recognize the privacy impacts brought forth by cellular telephone use within modern society and the government's use of these devices as a surveillance technology.

4. Fourth Amendment and Technology

The intersection of technology and privacy continues to evolve in part, because technology becomes part of the fact pattern under Fourth Amendment analysis. Individual expectations of privacy and society's acceptance of technology, regardless of individual expectations, are critical determinations under Fourth Amendment privacy analysis (*City of Ontario v. Quon*, p. 2629). Rather than focusing on the government's actions, privacy determinations by the courts focus on what the targeted individual knew, or should have known, regarding the expectation of privacy under a Fourth Amendment analysis (Freiwald, 2007, p. 22). Constitutional privacy decisions often become circular arguments, as identifying what society deems reasonable is determined by the same court that decides whether a search has occurred (Rubenfeld, 2008, pp. 106–107). Therefore, legal decisions on privacy will always lag behind the development and use of technology because the reasonable expectation of privacy is predicated upon the specific use of the technology and how that use impacts both the subjective and objective expectations of privacy (McCullagh, 2001, p. 140).[37] However, in that Fourth Amendment law is fact driven, the evolving nature of technology makes it more difficult to synthesize disparate technologies and fact patterns into a usable framework for guiding government to ensure the appropriate use of mass surveillance technology.

[37] For example, the U.S. Supreme Court did not review GPS technology used for surveillance until 2012, well after its general use within the public realm.

a. AFIS Evolution

Regarding the seminal biometric identifier, fingerprints, the U.S. Supreme Court ruled that the provision of fingerprints to the government was not a search given it was a minor governmental intrusion (*Davis v. Mississippi*). At the time of the *Davis* decision, which was prior to AFIS, fingerprint analysis was a labor intensive and time-consuming manual process subject to individual review of fingerprints (Wilson & Woodard, 1987, p. 13). AFIS automated the manual fingerprinting process, thereby allowing for the comparisons of thousands, if not millions of prints, in a short time, (Constance, 1995, p. 401). Today, the AFIS database contains over 60 million comparison fingerprints (Federal Bureau of Investigation, n.d.). Despite the vast amount of comparison data now available, and a more efficient process for the comparison of fingerprints, the technology did not create a Fourth Amendment issue.

However, the subsequent processing, retention, and use of the fingerprints, as biometric data, is distinct from the initial collection of the fingerprints. For example, an administrative requirement to fingerprint jurors raised issues regarding whether the fingerprinting of jurors was constitutional and whether the subsequent retention and use of those prints created a privacy invasion (*Goodman v. Liebovitz*). The Court held that mandatory fingerprinting of jurors was not a search or seizure under the Fourth Amendment (p. 506). However, the subsequent retention and use of those prints, (the data), after they served to verify the initial identification requirement, were not supported by law or policy (p. 507). Therefore, the court ordered their expungement or their return to the jurors (p. 507). In essence, the court distinguished the fingerprints, the data collection, from the subsequent retention and dissemination of fingerprints, and the Fourth Amendment privacy implications that attach.

If it is believed that history repeats itself, AFIS' evolution has lessons for today's use of surveillance technology. As a result of the technology advancements provided by AFIS, it became an important identification tool usable not only for criminal investigations, but also by other agencies, government and private (Constance, 1995, p. 403). The U.S. Supreme Court has ruled that efficiencies provided by enhanced technology do not automatically give rise to constitutional violations (*United States v.*

Knotts, p. 284). The social drivers for the expansion of the government's use of technology present today—resource scarcity, efficiencies, and advancing investigative practices—also drove the development of AFIS (Moses, 2012, chap. 6, p. 8). The back end issues of data storage and retention generated from the government's use of surveillance technologies continue to test traditional concepts of privacy, and as a result, the law lacks guidance on what constitutes privacy in a digital age (Solove, 2002, pp. 1217–1218). These same issues, data retention and subsequent use, were of concern when AFIS first rolled out. However, today, rarely is any thought given to the taking of or even subsequent use of fingerprints. Does society just "get over" privacy concerns as technology becomes more commonplace?

b. Today's Surveillance Technology

While *Olmstead*, *Davis* and *Katz* provide the foundation for Fourth Amendment analysis of surveillance technology's impact on privacy, these decisions do not address the government's mass monitoring of individuals' movement in public spaces. Even the Supreme Court has recognized that mass surveillance is different from other technology uses and may well require another type of analysis and/or decision framework (*United States v. Knotts*, p. 284). Privacy decisions involving surveillance technology contribute to the legal jurisprudence, but have limited scope in that they are often technology specific, as seen in the following review.

(1) *Berger v. New York.* The privacy impact of law enforcement' use of surveillance technology became part of the national discussion with two cases, *Berger v. New York* and *Katz v. United States*. The U.S. Supreme Court gave notice to Congress that electronic bugging, (*Katz)*, and electronic wiretapping, (*Berger*), would be reviewed in its upcoming term, and Congressional action on surreptitious surveillance would have to wait for the Court's decision in these cases (Kerr, 2004, p. 849). In part, it was the *Katz* decision that prompted Congress to enact legislative guidelines for law enforcement's use of surveillance technology, particularly as it applies to wire taps and overhears (*United States v. Jones*, pp. 962–963). Both decisions continue to have significant impact on law enforcement's use of surveillance technology even today.

(2) *Berger v. New York*. In *Berger*, the U.S. Supreme Court struck down a state law that allowed eavesdropping absent judicial oversight and without time controls as unconstitutional under the Fourth Amendment (*Berger v. New York*). Reaching back to 1862, the *Berger* Court analyzed the evolution of the law relative to eavesdropping and its progeny, which identified the growing ease with which technology allows access to private conversations (*Berger v. New York*, pp. 50–53). The government argues that striking down the state law would cripple law enforcement's ability to dismantle organized crime (*Berger v. New York*, p. 60). However, the U.S. Supreme Court held that the state statue authorizing law enforcement wiretaps for an unspecified duration and without judicial oversight lacked the procedural and legal safeguards required under the Fourth Amendment (p. 60).[38] The Supreme Court, in providing guidance to government on appropriate standards for wiretapping surveillance, outlined constitutional prerequisites, including:

- Judicial or neutral evaluation of the existence of probable cause;
- Specificity as to the crime committed, the place to be searched, and items or people to be seized;
- A termination date for the surveillance;
- Some form of notice or special circumstance to excuse notice; and,
- A return on the warrant (Kerr, 2004, p. 848).

Six months later, the Supreme Court decided *Katz*, and established the reasonable expectation of the privacy standard under the Fourth Amendment. Also under *Katz*, the U.S. Supreme Court affirmed that suppression remedies would be available to individuals subject to unlawful surveillance by the government (Freiwald, 2007, p. 51). Suppression remedies are a critical tool for defense and civil litigation, as they provide for sanctions, a remedy not present in other subsequent statutory enactments, such as ECPA (Freiwald, 2011, p. 681). Further, not only does *Berger* establish the need for proper judicial oversight of the government's surveillance of its

[38] In his dissent, Justice White commented on the contemporaneous Congressional action during the Supreme Court hearings on *Katz* and *Berger*, perceived to address what was thought to be a gap in law enforcement surveillance surrounding electronic surveillance, inclusive of wiretapping (*Berger v. New York*).

citizens, but also combined with *Katz*, both cases stand for the proposition that private conversations are protected under the Fourth Amendment.[39]

(3) Tracking Technology—*United States v. Knotts*. Technology's ability to assist law enforcement surveillance continues to evolve. In *Berger and Katz,* at issue was over hear technology. In *Knotts*, law enforcement's use of beeper technology for surveillance came before the Supreme Court. Beepers have become obsolete, as most law enforcement surveillance techniques now use satellite-based technology (Shah, 2009, p. 283). However, the framework for the court's analysis of the beeper surveillance technology continues to resonate within the Fourth Amendment doctrine. The issue before the *Knotts* court was whether the government's use of a beeper to track a moving vehicle on public streets and while parked at the driver's residence was a search under the Fourth Amendment (*United States v. Knotts*). Secreted by law enforcement inside an item placed by the respondent into his vehicle, the beeper emitted signals for up to three days that enabled the police to track and follow the vehicle (p. 278). The court identified that the beeper provided information on the travel of a vehicle about the public way (pp. 282–284). The Court held that beeper provided only a more effective means of observation of a vehicle about the public way, something already ruled to not implicate the Fourth Amendment (pp. 282–284). In holding that no search under the Fourth Amendment occurred, the court held that the technology merely augmented the sensory ability of the officers (pp. 284–285).

Knotts reflects the ambivalence of the Court in addressing the more fundamental privacy concerns raised by advancements in technology. The *Knotts* Court discusses, without resolution, whether continual mass surveillance under a dragnet-type law enforcement practice is subject to any differing constitutional analysis (*United States v. Knotts*, p. 284). Justice Stevens voiced concerns that the *Knotts*' decision would create confusion for subsequent Fourth Amendment review given that the use of electronic surveillance readily implicates privacy concerns that *Knotts* does not address (p. 288),

[39] The ensuing national debate over *Berger*& *Katz* contributed to Congressional enactment of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, (Title III), discussed herein pp. 118–121.

with Justice Stevens concurring. However, by narrowly defining the issue before the Court, the *Knotts* Court chose to ignore those privacy concerns not immediately before it (p. 284).

The reticence of the U. S. Supreme Court to address the overall privacy impact of surveillance technology used by the government to monitor the public movement of its citizens is repeated in subsequent cases, including its 2012 decision in *Jones*, and contributes to the ongoing uncertainty of the privacy boundaries under Fourth Amendment decisions involving technology. Even though the *Knotts* court recognized that the beeper technology did not implicate the Fourth Amendment, it gave voice to concerns over the greater levels of detailed information that technology allows (*United States v. Knotts*, p. 284). As a measure of quantity rather than just an issue of sense enhancement, the use of sensor surveillance technology may provide a need for greater constitutional protections (Hutchins, 2007, p. 440). However, the degree of intrusion or the quantity required to create differing constitutional review remains unanswered despite concerns raised in the public and by the Court itself. Fourth Amendment doctrine continues to analyze the use of each specific technology, rather than the privacy interest at stake, thereby failing to provide sufficient guidance to government for evolving technologies used for surveillance.

(4) *Kyllo v. United States*. In *Kyllo v. United States*, the issue before the Supreme Court was whether the government's use of infrared thermal imaging was a Fourth Amendment search (*Kyllo v. United States*). The technology was used from a public street to determine heat sources within the home (*Kyllo v. United States*).[40] Identifying thermal imaging as a form of sense enhancing technology, the Court held that its use would rise to a constitutionally cognizable search if the information derived from within the home were not possible without the technology (pp. 34–35). In that the normal senses could not detect heat within a home, the use of the technology to obtain information from within the home was ruled a search under the Fourth Amendment (p. 35).

[40] The distinction of use of technology outside the home harkens back to the decision in *Olmstead* in which no Fourth Amendment search was found to have occurred given government did not enter the home.

Kyllo demonstrates that place continues to weigh prominently in the Fourth Amendment privacy analysis. Enhanced privacy protections attach to the interior of the home (*Kyllo v. United States*, p. 40). The *Kyllo* Court held that to find differently would allow police technology to circumvent the intention of the Fourth Amendment's limitations on government intrusion into the private lives of its citizens (p. 34). Therefore, it is not only the technology used, but also where the government surveillance reaches that influences the Courts determination of whether a search for Fourth Amendment purposes occurred. In 1928, the Supreme Court Justice Brandeis opined that the Constitution must address what may be, not just what has been (Olmstead *v. United States*, p. 474). However, given the fact that driven analysis occurs under Fourth Amendment review, law enforcement is left to guess as to the appropriate standards and boundaries for evolving surveillance technology.

The role of technology and the expectations of society that result from its use remain hotly contested privacy issues. Defining Fourth Amendment privacy standards through the evaluation of specific technologies creates a tautology wherein the Court determines whether a reasonable expectation of privacy is anticipated by defining society's standards for use of that technology (Barrett, 2002, p. 23). However, dramatic technological change may lead to periods in which societal expectations regarding the use of technology and its relation to privacy are in flux (*United States v. Jones*, p. 962), with Justice Alito concurring. Ultimately, evolving technology may produce significant changes in privacy expectations and deciding such expectations ahead of the evolution presents challenges for privacy and use of evolving technology. If Fourth Amendment doctrine has not been able to provide and establish consistent standards for individual privacy protections and the government's use of surveillance within the last 94 years, it is time for a new direction?

5. The Privacy Challenge Given GPS and Evolving Technology

While technology may change, law enforcement's need to conduct criminal investigations remains. Under Fourth Amendment doctrine, the courts determine whether

the surveillance technology in use was sense augmenting,[41] identifying that if law enforcement was able to legally accomplish the action independent of the technology, then no search under the Fourth Amendment constitutional protections attach (Hutchins, 2007, pp. 434–435). GPS is one technology that law enforcement is increasingly using, given that it as an efficient and economical way of tracking suspects and developing evidence (Shah, 2009, p. 281). However, GPS technology provides more information than just route and location information. GPS allows government to amass individual, discrete data such that a broader, more descriptive, and therefore intrusive, set of data results (*United States v. Maynard*, pp. 561–562).

GPS facilitates tracking surveillance in a manner consistent with beeper technology. However, it also is capable of providing significantly augmented data, which has the ability to generate a mosaic of information regarding the private life (*United States v. Maynard*, pp. 561–562).[42] In part, the prevalence of GPS in modern society also contributes to the growing privacy concerns over data aggregation and mass monitoring by the government.

a. Case Law Approach to Addressing Government's Use of Sensor Technology Surveillance

Despite the prevalence and use of sensor technology by the government to conduct mass monitoring of its citizens, minimal legal guidance exists. Much of the existing doctrine has evolved over time because of various judicial decisions addressing the government's use of technology to conduct surveillance. The challenge with a case law-based doctrine is that it is slow to develop and is factually driven, which results in incremental change and sometimes seemingly conflicting decisions based on the facts presented to the court. However, the social use and acceptance of technology is moving at a rapid pace. Awaiting legal decision on the use of technology is neither practical nor

[41] Generally, sense augments refers to "extrasensory" tools, electronic or scientific that allow law enforcement to gather information beyond that capable through an individual's normal human senses (Webb, 2011–2012, p. 760).

[42] Under the mosaic theory, disparate items of information, while of little value individually, take on added significance when combined with other items of information, thereby creating a sum greater than its parts (Pozen, 2005, p. 630).

beneficial, as technology develops rapidly and is quickly introduced into society. Law enforcement has been using GPS for over two decades, yet the Supreme Court did not accept review of the government's use of the technology until 2012.

The legal validity of the government's use of sensor technology, namely GPS, to conduct surveillance came to a head when the U.S. circuit courts of appeals split as to whether the use of GPS constituted a search under the Fourth Amendment.[43] The *Jones* case generated interest within both law enforcement and civil advocacy groups because it was the first time the Supreme Court was to address the use of GPS by law enforcement to conduct surveillance.

What was seen as the controlling law by some courts, *Knotts*, held that the use of a tracking device by the government to conduct surveillance of a vehicle upon the public way was not a search for Fourth Amendment purposes (*Knotts*, 1983, p. 284). The law was settled that no reasonable expectation of privacy is anticipated for a vehicle operating on the public way given the public exposure of the vehicles and their movements (Kerrane, 2011, p. 1723). However, the technology in question in *Knotts* was a beeper tracking device and not GPS, which had not yet been addressed by the U.S. Supreme Court. Therefore, the lower courts were left to interpret the application of the provisions of the Fourth Amendment to the government's use of GPS to conduct surveillance.

b. A Split of Circuit Court Opinion

(1) *Knotts* as Controlling the Issue of GPS Surveillance by Law Enforcement. In addressing the issue of law enforcement using GPS to conduct surveillance, the 7th, 8th and 9th Circuits identified *United States v. Knotts* as controlling. These circuits held that use of GPS by law enforcement for surveillance of an individual was not a Fourth Amendment search in that it merely obtained information that would

[43] The 94 U.S. judicial districts are divided into 12 regional circuits, each with a court of appeals. A court of appeals hears appeals from the district courts located within its circuit, including appeals from decisions of federal administrative agencies. The Court of Appeals for the Federal Circuit has nationwide jurisdiction to hear appeals in specialized cases, including patent laws and cases decided by the Court of International Trade and the Court of Federal Claims (United States Courts, n.d.).

otherwise be available to law enforcement, namely the travel of the vehicle upon the public way (*United States v. Cuervas-Perez*; *United States v. Marquez*; *United States v. Pineda-Moreno*).

(2) *United States v. Cuervas-Perez*. Within the 7th Circuit, in *United States v. Cuervas-Perez*, the court held that the government's use of GPS to conduct a surveillance of a person was not a search for Fourth Amendment purposes (*United States v. Cuervas-Perez*, pp. 273–274). The *Cuervas* court acknowledged the holding of the D.C. Circuit's decision in *Maynard*, but distinguished its decision. The *Cuervas* court followed the precedence of the *Knotts* decision, in holding that vehicles that travel upon the public way have no expectations of privacy and are subject to lesser Fourth Amendment protections (*United States v. Knotts*, pp. 281–282). Noting the privacy concerns over the real-time information provided by GPS, the court identified that the technology did not create the information, but drivers did so by driving upon the public roads (*United States v. Cuervas-Perez*, p. 274). Noting that the GPS device was installed on the subject's vehicle while upon the public way and that the 60 hours of surveillance was not of sufficient length to expose the individual's otherwise private activity, the court held no Fourth Amendment privacy implications arose from the government's use of the GPS surveillance (p. 274). In essence, the *Cuervas* court maintained that just because the GPS made the government's surveillance more efficient, it did not invoke Fourth Amendment privacy concerns because the use of the GPS was not a search.

(3) *U.S. v. Marquez*. In *U.S. v. Marquez*, the 8th Circuit followed *Knotts* in holding that the government's use of GPS to conduct surveillance of a vehicle moving about the public way did not implicate Fourth Amendment privacy concerns (*United States v. Marquez*, p. 610). The GPS device was attached to the individual's vehicle while parked in a public parking lot, relayed information for a period of slightly less than five months and could only transmit information while outdoors (p. 607). The court held that the police had a reasonable suspicion that the vehicle tracked was involved in the interstate transport of drugs and the use of the GPS device merely allowed the police to conduct lawful surveillance more efficiently (p. 610). While noting

privacy concerns raised about government's ability to engage in "wholesale surveillance," *Marquez* stated the installation and use of the GPS device was neither random or arbitrary, and, therefore, such concerns did not play into the facts before the court (p. 610).

(4) *United States v. Pineda-Moreno*. In *United States v. Pineda-Moreno*, the 9th Circuit was not concerned over the length and duration of the government's surveillance. Rather, the court defined the issue as whether the placement of the GPS device on a vehicle parked on the public way invoked privacy protections under the Fourth Amendment (*United States v. Pineda-Moreno*, p. 1213). The government's GPS surveillance of the subject lasted for a period of four months (p. 1213). The court followed the precedence of *Knotts*, holding that the government obtained information about the subject's travel along the public way, and therefore, no search for Fourth Amendment purposes occurred (p. 1216).[44]

The *Cuervas, Marquez* and *Pineda-Moreno* courts analyzed the government's use of GPS to conduct surveillance through a focus on how and where the technology was installed, and how it tracked the movement of the vehicle under surveillance, thereby representing a very physical focus for Fourth Amendment search determinations despite increasing virtual implications (*United States v. Cuervas-Perez*, pp. 273–273; *United States v. Marquez*, p. 601; *United States v. Pineda-Moreno*, 2010, p. 1217). While these courts raised the possibility of differing analysis under the Fourth Amendment should the government surveillance arise to the level of mass surveillance of the movement of vehicles upon the public way, none ruled on the issue. Further, the issue was narrowed, with the courts focusing on how and where the surveillance was conducted, that of movement upon the public way, rather than on the detailed information of time, space, and location that GPS provides.

[44] It should be noted that on February 12, 2012, the U.S. Supreme Court vacated the judgment against *Pineda* and remanded the decision back to the 9th Circuit for further review in light of the decision in *U.S. v. Jones*. The U.S. Supreme Court made no further comment (See *Pineda-Moreno v. United States*, 132). Upon remand, the 9th District held that suppression was not warranted because the agents objectively relied on then-existing binding precedent when they approached Pineda–Moreno's Jeep in public areas, attached tracking devices to it, and used those devices to monitor the Jeep's movements (*United States v. Pineda-Moreno*, 688).

(5) *U.S. v. Maynard*. The D.C. Circuit split from the other circuit courts of appeals in identifying that *Knotts* was not dispositive when faced with GPS surveillance conducted by the government. The *Maynard* court conceded that *Knotts* was controlling for government's surveillance of a vehicle moving about the public way (*U.S. v. Maynard*, pp. 563–564). However, the *Maynard* court defined the issue before it as one of first impression, noting that the Supreme Court has not answered the issue as to whether "mass" electronic surveillance requires a warrant (p. 558).

In *Maynard*, the court focused on the depth and length of surveillance, rather than how the technology was attached or where it tracked the vehicle under surveillance (*United States v. Maynard*, pp. 557–558). Called into question was whether the issue was government-conducting surveillance of that which was in the public view as opposed to the whole of the information; the mosaic that GPS provides to the government (pp. 562–563). The court noted that a reasonable person does not expect individuals to be able to monitor continuously their every movement in a vehicle, including route, length, location, stops, and duration of those stops over a period of 28 days, as occurred within the case before it (p. 558). As such, the 6th Circuit held that the use of GPS by the government to conduct surveillance was a search under the Fourth Amendment and its warrant requirements attached (p. 563). The split among the Circuit Courts of Appeals as to whether the government's use of GPS to conduct surveillance constitutes a search under the Fourth Amendment set the stage for Supreme Court review of the matter.[45]

(6) *Jones v. United States*. The Supreme Court accepted review of the issue in *Jones v. United States, (Maynard),*[46]whether law enforcement's use of GPS to conduct surveillance was a search for purposes of the Fourth Amendment, and

[45] Supreme Court Rule 10 provides that review on a writ of certiorari is not a matter of right, but one of judicial discretion. A petition for a writ of certiorari will be granted only for a compelling reason. Including in the Court's authority is the review of those cases where a U.S. court of appeals has entered a decision in conflict with the decision of other U.S. courts of appeals on the same important matter (S.Ct. Rule 10. 2010).

[46] *U.S. v. Jones* was a consolidated case, originally named *U.S. v. Maynard*. However, the conviction of the defendant Maynard was upheld by the D.C. Circuit Court of Appeals while the defendant Jones' conviction was overturned as a result of the GPS claim. The government sought writ of certiorari from the U.S. Supreme Court only as to Jones and the issue of whether GPS is a search for Fourth Amendment purposes.

decided the case on January 23, 2012 (*United States v. Jones*). The Court unanimously held that the government conducted a search for purposes of the Fourth Amendment when it attached a GPS tracking device to the property of the subject under investigation (*United States v. Jones*).[47] The majority opinion, authored by Justice Scalia, identified the property interest as controlling in determining whether a Fourth Amendment search occurred (p. 953). The Court held that the government conducted a search in attaching the GPS device to the personal property of the subject under investigation with the intent to collect information and actually having collected information (pp. 948, 952).

In relying upon traditional trespass theory as a threshold issue to resolve whether the use of GPS in *Jones* was a search under the Fourth Amendment, the Supreme Court avoided having to answer as a matter of law whether the government's use of mass surveillance invokes Fourth Amendment privacy concerns (Hutchins, 2012). The Supreme Court left open to subsequent review whether it is constitutional for the government to track an individual's movement for a period of time as long as no physical trespass to individual's property occurs (Rosen, 2012). As a result, despite being the first Supreme Court decision on GPS surveillance by the government, *Jones* provides minimal guidance to law enforcement on the appropriate boundaries under the Fourth Amendment for the use of sensor surveillance technology.

Somewhat equivocally, the majority opinion also held that the reasonable expectations test, the *Katz* standard, remains valid law (*United States v. Jones*, pp. 952–953). Absent the threshold trespass by the government, the foundation for the *Jones* decision, the Court held that governmental surveillance without trespass would remain subject to a *Katz* analysis (p. 953). However, the Court failed to further define the reasonable expectations of privacy in a digitized world, and therefore, the distinctions are left for the lower courts to work out.

The *Jones* court did hold that the *Katz* reasonable expectation of privacy test is an expansion of, rather than a substitute for, the common-law trespassory

[47] Justice Scalia wrote the majority opinion of five justices. Justice Sotomayor joined the majority opinion but also wrote a separate concurring opinion. Justice Alito wrote a concurrence, but only in result, and was joined by Justices Breyer, Ginsburg and Kagan.

test (*United States v. Jones*, p. 952). However, it failed to address remote, e.g., non-trespassory surveillance, and as a result, the critical privacy inquiry remains—does the government's expansive use of pervasive, mass surveillance of its citizens movement upon the public way overcome reasonable expectations of privacy? How *Jones* impacts subsequent legal review of the government's use of sensor technology to conduct surveillance remains uncertain. In part, the decision in *Jones* reaffirms that location remains a critical reference in determining the constitutional protections afforded individuals (Gershman, 2010, p. 927). However, Justice Alito noted that the Court's decision would create vexing problems for courts reviewing future surveillance cases, particularly where the government's surveillance is remote, without physical intrusion upon the subject's private realm (*United States v. Jones*, p. 962), with Justice Alito concurring. The physical trespass doctrine, the basis for the Supreme Court's decision in *Jones*, fails to address the government's ability to conduct GPS surveillance when the GPS is carried by the party being tracked—namely through cellular telephone technology or as a result of an event data recorder, (EDR), technology in automobiles[48] (The Editorial Board, 2013).

As a result of the Supreme Court's narrowing of the privacy issue before it, rather than examining the privacy impact of the expanding use of pervasive mass surveillance technology by government, the gap between privacy protections and the government's use of surveillance technology will continue to grow. The Supreme Court justices failed to define where and when Fourth Amendment constitutional triggers occur, despite noting that for most offenses, longer-term GPS surveillances may impinge upon constitutional expectations of privacy (Clancy, 2012, pp. 312–316). The disinclination of the Supreme Court to address the general privacy concerns raised by the government's use of GPS to conduct surveillance is even more perplexing given the concerns noted within the majority and concurring opinions over the privacy impact of surveillance technology used by the government (*United States v. Jones*, p. 954), with

[48] Over 96% of vehicles now have EDRs, (black boxes), which include GPS technology. However, the law is all over the place as to who can access the information and when, with only 13 states having laws. The Senate introduced a bill to mandate their installation in all vehicles, yet does little to address the privacy concerns raised by the data, which is not considered to be owned by the vehicle owner.

Justice Sotomayor concurring (pp. 956–957), and Justice Alito concurring (pp. 961–963). In failing to provide legal guidance and a framework to address the broader privacy issues triggered through the government's use of surveillance technology, and not just identifying vague concerns, the *Jones* Court merely kicked the can—or the sensor—down the road.

6. Evolving Body of Local Law

In the absence of specific legal guidance, privacy protections afforded U.S. citizens are becoming an issue of local geography rather than consistent legal policy. Unlike the U.S. Supreme Court, lower courts have been more aggressive in defining legal parameters for the government's use of GPS to conduct surveillance and its implications for privacy. In light of the refusal of the U.S. Supreme Court to establish the legal parameters for the government's use of GPS surveillance in *Jones*, lower court decisions will continue to drive the legal privacy protections for individuals subject to the government's use of mass surveillance technology. These decisions continue to come before the courts, with somewhat varying outcomes, as noted below.

a. People v. Weaver

In a pre-*Jones* decision, in *People v. Weaver*, the New York state's highest court addressed whether the use of a GPS device attached to the vehicle of the subject under surveillance for a period of 65 days constituted a search (*People v. Weaver*, p. 1201). The court found the government's prolonged use of a GPS device to conduct surveillance to be a massive invasion of privacy, and as such, surveillance is inconsistent with even the slightest reasonable expectation of privacy (p. 1201). The *Weaver* court identified concerns over the lack of judicial oversight for the "dragnet use" of the technology that allowed access to intimate details of daily life at the sole discretion of law enforcement (p. 1203). Unlike the U.S. Supreme Court, the state court identified that 26 years after *Knotts*, GPS technology forces the issue of whether twenty-four hour surveillance of any citizen were possible without judicial oversight (p. 1200). While recognizing the area remains unsettled as a matter of federal constitutional law, the *Weaver* court held that the state of New York's constitution provides greater privacy

protections for its citizens, independent of any federal Fourth Amendment application (p. 1202). *Weaver* demonstrates not only the different outcomes possible under traditional Fourth Amendment privacy analysis, but also the willingness and capacity of state courts to expand privacy protections to its citizens independent of the federal constitution.

b. U.S. v. Skinner

Within the 6th Circuit, pursuant to *United States v. Skinner*, no Fourth Amendment implications arise from the government's use of the GPS located within the cellular phone of an individual tracked by the government (*United States v. Skinner*, p. 777). In *Skinner*, the government obtained an order from a federal magistrate judge authorizing the release of subscriber information, cell site information, GPS real-time location, and "ping" data for the individual's phone, and tracked the individual for a period of several days through several states (p. 776). Identifying the phone was a tool used in the furtherance of criminal conduct; the court held that no reasonable expectation of privacy is anticipated, despite the defendant's stated expectation that the phone was not traceable by law enforcement (p. 777). In a nod to *Knotts*, the court noted that physically tracking a defendant and tracking him via cell phone GPS technology offers no constitutional difference (p. 778). The *Skinner* court held that law enforcement tactics must be allowed to advance with technological changes to prevent criminals from circumventing the justice system using technology (p. 778).

In distinguishing its decision from that of the Supreme Court in *Jones*, the *Skinner* court noted that the defendant obtained the cellular telephone for the purpose of communication (*United States v. Skinner*, p. 781); unlike the action in *Jones* where the police physically occupied private property to place a GPS unit on the individual's property, and the individual's phone already included the GPS technology used to track the phone's location (p. 781). The government used a known telephone number to track the device while it travelled upon public thoroughfares; therefore, the court ruled that *Skinner* did not have a reasonable expectation of privacy in the GPS data and location of his cell phone" (p. 781). As a result, the use of cellular telephone GPS signals to track the location of a cellular telephone, and, ostensibly an individual, does not constitute a search

within the 6th Circuit. In this post-*Jones* decision, the legal focus remains on the level of governmental intrusion, and whether a reasonable expectation of privacy is anticipated.

c. U.S. v. Nowka

In *U.S. v. Nowka*, the defendant moved to dismiss video surveillance obtained as the result of the government's installation of a camera upon a utility pole that allowed the camera to be aimed at the defendant's property (*United States v. Nowka*). Relying in part upon the Supreme Court's decision in *Jones*, the claim before the court focused on the trespass from the installation and retrieval of the camera and the pervasive, 24 hour surveillance capacity of the surveillance camera (*United States v. Nowka*). However, the district court held that no governmental trespass occurred as no proof existed that the pole on which the camera was installed was either owned by the defendant or was on his property (*United States v. Nowka*). As a result, pursuant to *Katz*, the *Nowka* court held that no reasonable expectation of privacy was anticipated given that the camera took pictures of an area plainly visible to anyone (*United States v. Nowka*).

Unlike the issues raised in the D.C. Circuit Court of Appeals decision in *Maynard*, the *Nowka* court did not address, nor was it concerned with, the length of the camera surveillance. Rather, the *Nowka* court analogized the camera surveillance before it to the surveillance conducted in *Florida v. Riley* (*United States v. Nowka*). In *Riley*, the U.S. Supreme Court ruled that no Fourth Amendment protections attached to a party arrested after law enforcement discovered contraband in a field by flying a helicopter over the individual's property (*Florida v. Riley*, p. 445). Rather than delve into the privacy concerns raised by technology, the *Nowka* court decided the issue before it pursuant to traditional Fourth Amendment doctrine in focusing on how the GPS device was installed and how the government obtained the information rather than the breadth and duration of the government's surveillance.

As evidenced by the *Skinner* and *Nowka* decisions, the precedential guidance of *Jones* does not dispose of the issues raised by pervasive surveillance. In fact, Justice Alito notes that the Court's decision in *Jones* fails to provide sufficient guidance for subsequent cases wherein the government uses technology that provides the ability to

conduct surveillance without trespass (*United States v. Jones*, p. 955). In a pre-computer age, the privacy protections of the Fourth Amendment were based upon practical considerations (*United States v. Jones*, p. 963), with Justice Alito concurring. However, attempting to analogize surveillance technology to physical intrusion, which is the precedential focus of Fourth Amendment doctrine, creates problems in logic given the mass amounts of minute data that can be obtained without physical intrusion (pp. 956–957), with Justice Sotomayor concurring. This issue, tying Fourth Amendment jurisprudence to a physical standard in a digital era, was a specific concern of five of the nine Supreme Court justices in *Jones*. See *United States v. Jones*, with Justice Sotomayor concurring (pp. 955–957), and Justice Alito concurring (pp. 961–963), and but for Justice Sotomayor's identification of trespass as a constitutional minimum standard for determining the government conducted a search, thereby joining in the majority opinion, the decision in *Jones* may have been different (pp. 954–955), with Justice Sotomayor concurring. Accordingly, the precedential value of Jones will continue to be refined within the decisions of lower courts.

In addition to limitations caused by courts narrowing the privacy issues addressed under fact-based decisions, the case law approach is also temporally limited. It takes years to resolve a constitutional challenge to an alleged privacy violation; the GPS device at issue in *Jones* was attached to the vehicle in 2005 (*United States v. Jones*, p. 948). However, the pace at which technology is developed and introduced within the United States far outstrips the leisurely pace of fact driven case law. Pending definitive legal resolution of the appropriate boundaries for the use of surveillance technology, users and providers of new technology suffer from a lack of certainty, not only in data privacy, but also in the use and procurement of the technology involved (Elaluf et al., 2011, p. 6). Therefore, the risks in adopting new technology without clear guidance on privacy or legal restrictions will continue to be a barrier to effective and appropriate governmental use of sensor technology to conduct surveillance.

Ultimately, the challenge in defining privacy via constitutional legal review is that while the courts debate the meaning of words, privacy is an area of emotion and inherent right (Solove, 2010, p. 1513). As noted in *Jones*, the legislature can more

rapidly and ably respond to changing public attitudes regarding technology and craft the delineations that appropriately balance privacy and public safety in a timely, comprehensive way (*United States v. Jones*, p. 964), with Justice Alito concurring. The balancing of interests, privacy, and public safety, through clear and comprehensive legislative guidance, would better serve both public safety and personal civil liberties.

7. Statutory Response to Technology Surveillance

No comprehensive statutory protection for privacy exists within the United States and, as a result, a gap occurs in the protection for citizens from governmental intrusion into the private realm (Solove, 2010, p. 1517). As information becomes more digitized, the third party doctrine and the lesser protections afforded transaction data as opposed to communications data allow for significant privacy intrusions (Bagley, 2011, p. 167). However, Americans are increasingly using cloud computing and other private sector service providers to create, store, and publish their personal papers and effects, thereby increasing reliance upon third parties for the storage of their personal information (pp. 154–155). While the courts have held that automation of manual processes are not constitutional issues, Fourth Amendment doctrine continues to review privacy issues involving technology within a quaint perspective and fail to address the privacy implications that digital information brings forth, as compared to paper documents. The existing patchwork of state and federal statutory laws does not cover this gap nor do it fully protect individual privacy.

Existing statutes that address privacy are incomplete and do not cover privacy as a single issue. The U.S. Supreme Court noted that the United States is a society that chooses to dwell in reasonable security and freedom from surveillance (*United States v. Knotts*, p. 282). However, in contrast to the most of the developed world, the United States has no strong, comprehensive law protecting privacy (Stanley & Steinhardt, 2003, p. 15). Given the adherence to the third party doctrine by U.S. courts under the Fourth Amendment, only limited protections exist for digital records, and, therefore, privacy protections for electronic communications generally come from statutory protections (Computer Crime and Intellectual Property Section (CCIPS), 2009, ch. 1B3). Statutes do

provide two advantages over Fourth Amendment constitutional law—they can be drafted to delineate protections and consequences specifically for the failure to adhere to the statute and they may be drafted to apply to specific interests, such as directing the actions of private parties. However, in that many of the existing legislative privacy statutes were adopted in response to specific privacy concerns, privacy statutes vary significantly in the protections offered to individuals (Bergelson, 2003, p. 392).

New surveillance technology often generates a legislative reaction as privacy concerns grow. Statutory regulations amongst the different jurisdictions vary, thereby resulting in a lack of consistent guidance over government surveillance or clear protection for privacy (Helft & Miller, 2011). Legislation driven in response to a specific technology fails to provide guidance for current and future privacy issues, which results in a continuously reactive response to new privacy intrusions. For example, arising from the disclosure of Judge Robert Bork's video rental choices during his Supreme Court confirmation battle, video records are now protected through The Video Privacy Protection Act of 1988 (codified at 18 U.S.C. § 2710 (2002)) (Electronic Privacy Information Center, 2011). However, in 2012, many consumers no longer rent movie videocassette tapes, as identified within the act. Rather, they use the Internet to obtain their movie via a download—something not envisioned or addressed under the Video Privacy Protection Act. A limited legislative intent results in limited privacy protections, as a review of some of the key privacy statutes demonstrates.

a. Federal Legislative Response to Law Enforcement's Use of Eavesdropping Surveillance—Title III of the Omnibus Crime Control and Safe Streets Act of 1968

One of the first statutes that addressed law enforcement's use of surveillance technology, the Title III of the Omnibus Crime Control and Safe Streets Act of 1968, ("Title III"), provides federal regulation and control over the surveillance of electronic communications (18 U.S.C. §§ 2510–2522). Title III demonstrates Congress' ability to create legislation that balances the competing interests of law enforcement investigative needs and civil liberty interests independent of the provisions of the Fourth Amendment. Title III operates as a comprehensive statutory framework that regulates

real-time monitoring of wire and electronic communications (Computer Crime and Intellectual Property Section (CCIPS), 2009, ch. 1B3). It also serves as an example of the strength of statutory authority limiting the government's use of surveillance technology and also its weaknesses from a privacy perspective.

The U.S. Supreme Court granted writ of certiorari to two cases involving the use of electronic surveillance by the government in 1967. Extensive Congressional hearings were ongoing during the *Berger* hearing before the Supreme Court (*Berger v. New York*, pp. 112–113). Granting writ of certiorari to *Berger* and *Katz* signaled Congress that legislative action would have to await the Court's decisions (Kerr, 2004, p. 849). The Supreme Court decisions in *Berger* and in *Katz* established constitutional limitations over the government's use of technology in wiretapping private communications (*Berger v. New York*; *United States v. Jones*, pp. 950, 959–960), with Justice Sotomayor concurring. Title III was Congress' legislative response to the Supreme Court decisions in *Berger* and *Katz* and remains valid law today. Title III addressed the constitutional standards established by the Supreme Court's decisions in *Berger* and *Katz* and provided legal authority to law enforcement to conduct wire surveillance while mandating rules of procedure that ensured the government's actions to specified standards.

When it comes to privacy protections regarding wiretapping surveillance, statutes provide the primary source of protection (Kerr, 2004, p. 850). Title III provides for a limited grant of authority to law enforcement to conduct electronic surveillance, provided adherence to the legislatively specified procedural requirements occurs as listed under 18 U.S.C. § 2516(1). Section 2518 delineates the mandated requirements for the safeguard of citizens subject to governmental surveillance of electronic communications, including the identity of the subject, the nature of the communication, the time provisions, the minimization requirement, the record keeping and warehousing provisions, and a notice requirement (Sheridan, 1975, p. 339). Title III also prohibits private citizens from access to and the use of certain electronic surveillance (18 U.S.C. §§ 2511, 2515). In enacting Title III, Congress ensured that the complex field of electronic

surveillance was not left to the Courts to govern through evolving case law and *stare decisis* (*United States v. Jones*, p. 963), with Justice Alito concurring.

Title III also ensures that the government adheres to consistent standards when eavesdropping on the communications of its citizens. In granting specific authority to law enforcement to conduct electronic surveillance, Congress pre-empted independent state legislation governing the surveillance of electronic communications, absent adherence to federal standards (United States Attorneys Manual (USAM), 1997). Title III mandates that wiretapping be limited to the investigation of serious crimes as delineated within the statute, and may be allowed under similar state laws, including murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in dangerous drugs or other felony crimes (18 U.S.C.A. § 2516(1) &(2)). The courts have found that in enacting Title III, it was Congressional intent that the use of wiretapping be reserved as an extraordinary investigative tool of last resort (*United States v. Giordano*). No wiretap order may be issued unless law enforcement can show that other investigative procedures have failed, are useless, or are too dangerous (18 U.S.C. § 2518(1)(c)). Finally, under Title III, law enforcement must always consider whether normal investigative procedures could be used as effectively and given the evidence obtained as a result of each succeeding wiretap (*United States v. Castillo-Garcia*). Congress has assumed the lead in addressing privacy concerns associated with wiretapping, and the deference of courts to Title III rather than constitutional law in deciding such cases confirms Congress' authority (Kerr, 2004, p. 840). Title III demonstrates Congressional authority to enact controlling legislation for governmental use of technology in conducting surveillance and could provide a model for addressing new surveillance technologies.[49]

However, Title III does not control the government's use of all electronic surveillance technology. Title III is a comprehensive statutory response to wiretapping, but it is limited in its privacy protections, as it only addresses a specific surveillance technology used by the government (*United States v. Torres*). As such, Title III serves

[49] In fact, the proposed ECPA 2012 Amendment is modeled after some of the requirements contained within Title III, as discussed herein and certain portions of the proposed GPS Act, as discussed herein.

limited purpose in addressing the government's use of surveillance technology developed since 1968, a significant gap given the explosive growth of sensor technology.

b. The Electronic Communications Privacy Act

In 1986, Congress amended Title III by enacting the Electronic Communications Privacy Act of 1986, (ECPA) (Electronic Communications Privacy Act of 1986, §§ 2510–2522, 2701–2712, 3121–3126). ECPA was Congress' attempt to address privacy in the digital age (Wells, 2009, p. 230). ECPA was intended to address the fact that no longer is personal information secreted behind closed doors as hard drives now serve as filing cabinets and personal computers now store massive amounts of personal information, inclusive of financial and medical records (Saylor, 2011, p. 2812). ECPA is a trio of laws: the Wiretap Act or Title III (18 USCA §§ 2510–2522), which governs the interception of the contents of electronic communications; the Stored Communications Act (18 U.S.C. §§ 2701–2711), which covers the disclosure of certain electronic communications, and the Pen Trap statute (18 U.S.C. §§ 3121–3126), which regulates the real-time collection of communications address information (Burstein, 2008, p. 185). However, as with Title III, ECPA is limited in its protections and is primarily aimed at technology used by the government for the surveillance of communications (Electronic Communications Privacy Act, 2011).

ECPA also applies to private entities (18 U.S.C. § 2510). Statutory restrictions on private parties are important as entities, such as third-party service providers, contribute to privacy concerns in a digital world, and particularly for stored and downloaded digital content. When a private party has been given information that the government seeks, the U.S. Supreme Court has been known to hold that no expectation of privacy exists under the Fourth Amendment (Kamin, 2004, p. 104). Therefore, private parties have the potential to circumvent constitutional limitations on government through the use of third-party communications services, such as Internet service providers, to facilitate governmental surveillance (Kerr, 2004, p. 872). In drafting ECPA legislation to ensure applicability to private parties, Congress attempted to address concerns over the role of private parties and data surveillance of U.S. citizens, albeit within certain limited

circumstances[50] (Kamin, 2004, p. 121). However, at least one court has held that the ECPA's concern for privacy extends only to government action and third-party service providers, such as ISPs, are free to turn stored data and transactional records over to nongovernmental entities (*United States v. Hambrick*, p. 507). Therefore, the application of ECPA is still evolving given the growth of electronic communications.

When enacted, ECPA extended protections to electronic communications that fell outside the existing statutory scope of Title III, and thereby, were without clear constitutional protections (Burnstein, 2008, p. 186). ECPA was drafted to include the Pen Trap Statute and the Stored Communications Act, in addition to the existing Title III, The Wiretap Act. Under ECPA, protected content includes any information concerning the substance, purport, or meaning of that communication as it applies to any wire, oral, or electronic communication (18 U.S.C. § 2510(8); EPIC, n.d.a.). Essentially, if an electronic communication is in transit from origination to destination, the Wiretap Act applies; if it address information, such as phone number, then the Pen Register Act applies, and if it is already in electronic storage, then the Stored Communications Act governs (Oyama, 2006, p. 503).

c. Pen Register Act

A pen register is a device that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that the pen register does not include the contents of any communication (18 U.S.C.A. § 3127 (3), (4)). Pen registers record addressing information, such as telephone numbers and do not collect the contents of communications (*United States v. New York Telephone Company*).

The U.S. Supreme Court has found that no reasonable expectation of privacy is anticipated in the information generated by a pen register (*Smith v. Maryland*, pp. 742–745). In *Smith*, the issue presented to the Court was whether the phone numbers generated from a pen register installed by government without a warrant should be

[50] For example, employers have wide discretion to monitoring employees email under the business use, consent and purpose exceptions of ECPA, and as a result, the greatest restraint on workplace monitoring of electronic communications is the employer's statement of what is their policy.

suppressed as evidence (p. 737). The defendant in question was accused of robbing someone and then repeatedly calling this individual subsequently (p. 737). The Supreme Court found that telephone subscribers do not harbor any general expectation that the numbers they dial will remain secret; as such information is routinely used and disclosed to various parties within the context of normal business practices (p. 743). Absent a reasonable expectation of privacy in telephone numbers, no search for Fourth Amendment purposes occurred (p. 743).

Subsequently, other courts have expanded the application of *Smith* to e-mail and Internet users, finding that no expectation of privacy is anticipated for email addresses or the internet protocol (IP), addresses of websites visited, because the information is provided to and used by Internet service providers as a matter of routine business. For example, in *United States v. Forrester,* the 9th Circuit analogized the government's use of a pen register to capture email address information or IP addresses of websites visited through an Internet service provider to *Smith* and held that such use was not a search (*United States v. Forrester*). In *Forrester,* the government used information captured from a pen register installed through a service provider to capture email address information, the IP addresses of websites visited, and the overall account volume (p. 505). Therefore, the *Forrester* court held that the government's access to such information does not implicate the Fourth Amendment because users have no reasonable expectation of privacy in such addresses (p. 509). The court found the use of email addresses indistinguishable from the use of telephone numbers, and identified that the voluntary relay of contact number information through a third party negated any general expectation that the numbers, or email addresses, will remain secret (p. 510).

The Pen Register Act does not translate fully to digital address tracking, but share similarities in that they represent addressing information to which content is delivered to another address, be it telephone or email. In that the Supreme Court has not definitively ruled on the protections afforded email addresses and IP addresses, what, if any, protections apply are left for the courts to interpret and determine. However, ignoring the growth of social connectivity in digital space, the result of a rigid adherence to the third-party doctrine, would fail to provide Fourth Amendment privacy protections

for a significant component of daily life (Strandburg, 2011, pp. 614, 639). Therefore, ECPA's application to email addresses supports modern communication practices.

d. Stored Communications Act

The Stored Communications Act, (SCA), addresses the government's access to data already generated and held, regardless of how stored (EPIC, n.d.a.). The SCA was originally established to regulate electronic mail and data transmissions and remote computer processing and data storage (Robison, 2010, p. 1205). The SCA Act regulates government access to transaction records, in part by requiring a subpoena for access to subscriber information (18 U.S.C. §§ 2701–2712). However, the SCA does not require a warrant to access all stored data, thereby creating privacy problems within the modern context (Strandburg, 2011, p. 645). The 1980s technology, when SCA was enacted, differs significantly in comparison to the explosion of email, social networking and other communication technologies now available and in widespread use.

The courts are left to determine the outcome of the intersection of the SCA and third party doctrine as it applies to Internet communications. Some courts have ruled that customers of communication service providers do not have a reasonable expectation of privacy in customer account records maintained by a third party (*United States v. Perrine*). In *Perrine*, the government used data collected through the identification of IP access attempts and other email addresses to obtain subscriber information in prosecuting the appellant for child pornography (p. 1199). In fact, the *Perrine* court has noted that every federal court that has reviewed the issue has held that subscriber information provided to an Internet provider is not protected by the Fourth Amendment's privacy expectation (p. 1205). While *Perrine* is in alignment with the Fourth Amendment's third party doctrine, little electronic communication occurs without involving a third party. In that most websites now require users to disclose PII to gain access to services, and subsequently, store both content and non-content user information without legal limitation, the third party doctrine creates significant privacy concerns in a digital age (Bagley, 2011, p. 167).

Other courts are noting that the provision of consumer location information to a cellular service provider is not necessarily a voluntary disclosure. *In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records*, the government sought disclosure of historical cell location information pursuant to the SCA, 18 U.S.C. §2703(d) and was appealing the denial by the magistrate judge (In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to Government, p. 305). The government argued that no warrant or subpoena was needed but rather a court order sufficed to obtain the records it sought, given that the records were kept in the regular course of business (pp. 307–308).[51] The 3rd Circuit found that the SCA standard required only specific and articulable facts showing that reasonable grounds existed to believe that the contents or record of a communication are relevant and material to an ongoing criminal investigation, which is a lesser standard than the probable cause required by the lower court (p. 313). However, the 3rd Circuit Court also found that cell phone customers have not voluntarily shared location information with a cellular provider in any meaningful way (p. 317). The court remanded the case back to the lower court to determine under articulable facts whether the government met the standards required within 18 U.S.C. §2703(d) (p. 317).

Recently, further legislative action was taken to amend ECPA under the Electronic Communications Privacy Act Modernization Act of 2012, (ECPA 2012). H.R. 6529(11th): ECPA 2.0 Act of 2012 was introduced on September 21, 2012 by Representative Lofgren (D-CA 16) and was referred to committee (Govtrack.us, 2012). On November 29, 2012, the Senate Judiciary Committee approved a modified version of the original submission under H.R. 2471,[52] which would require law enforcement official to obtain a warrant from a judge to access messages in individual email accounts,

[51] The 3rd Circuit noted the additional support of other magistrates in the denial of the government's access to the information, in the lower court's primary finding that the government must show probable cause for a § 2703(d) order and identification that the government has long been required to obtain court approval for the installation and use by law enforcement agents of a device enabling the government to record or track the movement of a person or thing (In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to Government, 2010, pp. 308–309).

[52] See, H.R. 2471. http://www.leahy.senate.gov/imo/media/doc/Leahy-Substitute-to-HR2471.pdf.

excepting certain exclusions (Savage, 2012). In part, update and clarification of the electronic communications protected under ECPA is needed so that law enforcement, communications service providers, and other communications vendors have clear guidelines and standards as technology advances amidst dated law and standards (Cheverie, n.d.). Most significantly, under ECPA 2012, Senator Leahy's proposed amendment would expand protection to all emails, whether stored online or off (Sledge, 2012). It would also protect information stored in the cloud, such as documents in Google Driveg (Sledge, 2012). As with ECPA in 1986, ECPA 2012 attempts to address privacy issues implicated as a result of modern communications technology.

ECPA was intended to protect against unauthorized interception of electronic communications (In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to Government, p. 313). However, ECPA fails to provide real protection for modern electronic communications, as a 1986 law is tracking 2012 technology (Sledge, 2012). ECPA still only applies to certain technologies and how the courts apply and interpret ECPA depends upon what type of information is sought and how old it is (Helft & Miller, 2011). Lesser protections for data in storage as compared to protections for data in transit, fail to account for today's digital processes and how communications occur on a daily basis (Freiwald, 2007, pp. 17–18). Government needs to obtain a search warrant, which requires a hearing before a judge with proof of probable cause that the targeted individual is engaged in criminal conduct only when it seeks to read e-mails that have not yet been opened by their recipient and are fewer than 180 days old (Savage, 2012). Those messages that the individual has read, and retains in an email account are afforded lesser protections (Savage, 2012). Additionally, no suppression remedies or penalties exist for the failure to adhere to ECPA standards (*United States v. Perrine*, 2008).

In part, the ECPA protections exist as they do because of how technology was used in the 1980s. Given the dearth of email inbox capacity, most email messages important to the reader were downloaded and stored on a hard drive, as opposed to today's expanded inbox capacity and use of cloud computing (Sledge, 2012). A court order or subpoena issued by a prosecutor will suffice for these types of messages (Sledge,

2012). Paradoxically, those messages opened and retained by the user are provided lesser privacy protections than those emails delivered and remain unread. Regardless, ECPA 2012 remains under legislative debate, as concerns are raised over identifying the appropriate balance between public safety and privacy, and the impact upon criminal investigations that higher standards for government access would create (Savage, 2012). As it stands now, absent statutory governance, the third party doctrine under the Fourth Amendment serves to limit reasonable expectations of privacy in electronic communications given that most, if not all, such communications are stored within a third-party process. However, as evidenced by Congress' legislative address of communications privacy through the enactment of Title III and ECPA, a legislative response can be an effective means by which to address privacy protections not necessarily inherent in the Fourth Amendment.

e. The Privacy Act of 1974

The Privacy Act of 1974, (The Privacy Act), governs the use and retention of PII by the federal government[53] (The Privacy Act of 1974). The Privacy Act requires an information privacy officer and limits the collection and use of PII by federal entities (The Privacy Act of 1974, 8 (u)). Under § 552a(b) of the Privacy Act, agencies are prohibited from disclosing to any person or other agency any PII record that is contained in a system of records by any means of communication, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains (*Bechhoefer v. U.S. Dept. of Justice*). However, law enforcement investigations are exempt from the disclosure restrictions, thereby allowing for broader collection and dissemination of PII within law enforcement (The Privacy Act of 1974, (b)). Therefore, if an individual is subject to criminal investigative focus through governmental surveillance, privacy protections decrease under the Privacy Act.

As with most privacy legislation in the United States, The Privacy Act's jurisdiction is limited. The Privacy Act governs PII data processed and collected by the

[53] The Privacy Act, albeit by reference, unambiguously defines the term "agency" as an agency of the federal government under Section 552(f) despite a broader reference under section 7(b) (*Schmitt v. City of Detroit*).

federal government and does not directly apply to collection or use by local governmental or private entities (Shaffer, 2000, p. 28).[54] Given that law enforcement investigations are exempt from the PII collection and communication standards of the Privacy Act, it has minimal impact on data derived from law enforcement surveillance (The Privacy Act of 1974, 8 B iii & (j) 2). Since the Privacy Act has minimal impact on local law enforcement, a significant user of mass surveillance technology, it provides little real privacy protection for the expanded collection of PII data through the use of pervasive, mass surveillance technology.

However, the Privacy Act does provide guidance as to those PII data collection practices deemed appropriate by Congress. Under The Privacy Act, agencies may only maintain PII relevant and necessary to accomplish a required purpose of the agency (The Privacy Act of 1974, (e)(1)). Agencies maintaining PII are required to establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records (The Privacy Act of 1974, (e)(10)). Disclosure of PII record information without the individual's consent is prohibited, absent certain codified exceptions, e.g., use for research, criminal investigation or tax purposes (The Privacy Act of 1974, (b); *Alexander v. F.B.I.*).

f. The Geolocation Privacy and Surveillance Act

In keeping with the seemingly past practice of using legislation to address privacy concerns brought forward by a specific technology, a bill is pending before Congress that addresses the government's use of GPS technology for surveillance. The Geolocation Privacy and Surveillance Act (GPS Act, 112th Congress (2011–2012) S.1212 and H.R. 2168),[55] was first introduced in June 2011, and seeks to establish clear guidelines for governmental and private use of geolocation information (GPS Act). Thus far, the GPS Act has failed to gain legislative traction and remains inactive within

[54] The Privacy Act may have some application to local government, as distilled through local participation in fusion centers, federal task forces or through certain federal grant requirements under 28 C.F.R.§23, but is not an area of review within this thesis.

[55] Senator Ron Wyden (D-OR), the lead Senate sponsor of the legislation, identifies the need for legislation because the government is trying to "race a technological Indy 500" with laws "out of the horse-and-buggy era" (Anderson, 2011).

subcommittee, despite a recent attempt to amend the Cybersecurity Act of 2012, (S. 3414), with provisions of the GPS Act, (S.AMDT. 2688) (GPS Act).[56]

The GPS Act calls for enhanced oversight of government surveillance by requiring law enforcement to obtain a warrant from a judge before conducting GPS-enabled surveillance (GPS Act §2602(h); GPSGov, 2011). As with Title III, under the GPS Act, for law enforcement to obtain geolocation data from a variety of electronic devices, including cellular telephones, probable cause would be needed to obtain a judicial warrant to access geolocation information (GPS Act, §2601(5); Anderson, 2011). The GPS Act would also remove the legal distinctions, and differing privacy protections, between stored and real time location data (Granick, 2011). Despite the arbitrary distinctions made under ECPA, both types of data are significant sources of information (Granick, 2011). Furthermore, under §2605, the GPS Act holds private entities accountable for data disclosures and allows a right of civil action for those whose privacy rights have been violated in contravention of the GPS Act (GPS Act, §2605).

In the recent decision in *Jones*, the U.S. Supreme Court declined to define constitutional parameters for law enforcement's use of GPS in conducting surveillance of U.S. citizens. As a result, lower courts and state legislatures will continue to parse out the boundaries for permissible use of GPS by the government. Given the mobility of U.S. society, the GPS Act would ensure a consistent set of rules of engagement for law enforcement and ensure that privacy protections against persistent governmental surveillance through GPS are not based upon geography. However, while the GPS Act includes key protections for privacy, as with Title III, should the GPS Act become law, it will only address a specific surveillance technology in use by the government, namely GPS. Yet, in the absent of judicial direction and despite its focus on one technology, the GPS Act is one method to provide guidance to law enforcement and to protect individuals from the indiscriminate use of GPS surveillance by the government.

[56] The GPS Act has failed to gain traction and remains inactive within subcommittee, despite a recent attempt to amend the Cybersecurity Act of 2012, (S. 3414), with provisions of the GPS Act, (S.AMDT. 2688) (GPS Act, 2011; Walton, 2012). Whether the bill will be reintroduced remains to be seen.

g. The Gap

The existing statutory scheme that seeks to protect the privacy of U.S. citizens has proven to be anemic. As pervasive surveillance and mass aggregation of the derivative data grow, so will the uncertainty about when and how the law protects individual privacy interests. Absent a comprehensive statute on data privacy, the piecemeal approach to legislative protections will continue, with little real protection afforded to individuals in a digital age. The courts have proven to be either incapable or unwilling to address the privacy implications of mass surveillance by the government, as recently reinforced by the U.S. Supreme Court's failure to identify the constitutional limitations for the government's use of sensor technology to conduct surveillance in its decision in *Jones*. Further, the Supreme Court willingly signaled that Congress, more so than the courts, should address the issue given it has the ability to better respond to privacy issues raised as a result of rapidly changing technology (*United States v. Jones*, pp. 963–964), with Justice Alito concurring. Unlike the courts, legislatures can experiment with different rules and make changes when necessary based upon outcomes, both anticipated and unanticipated (Kerr, 2004, p. 871). A comprehensive federal statute addressing data privacy protections, rather than continuing to legislate the government's use of a single technology, will serve to protect privacy in accordance with the civil liberties guaranteed Americans.

h. Statutory Data Privacy Protection

Statutory data privacy protection is not without foundation. Unlike the United States, the rest of the developed world engages in strong comprehensive privacy laws (Stanley & Steinhardt, 2003, p. 15). Further, within the United States, little to no individual privacy protection is in place for the use and subsequent re-use of PII data, particularly for non-governmental users of such data. People are increasingly spending their lives in digital space, knowingly and unknowingly, exposing their personal details and images to constant recording by a great number of sensor devices, both private and government owned (Bignami, 2007, p. 235). Does convenience inevitably become a trade off for privacy such that it changes the shape of expectations of privacy? (*United States v.*

Jones, p. 963). Within this technology-rich society, millions of pieces of PII data are created, stored, and searched with great ease (p. 963). A variety of technologies within widespread use, from RFID toll transponders to cellular telephone location data, maintain PII as a routine business matter, and little legal control is exercised over the subsequent storage and reuse of the PII data generated. Given the increasingly blurred lines between public and private information, a data protection act would serve the interests of both government and individuals in identifying clear and consistent guidelines for data use, access, retention, and dissemination.

Clear and comprehensive federal legislation regulating the privacy rights and responsibilities of government, individuals, and commercial enterprises that collect PII is needed due to the development of privacy laws in the international arena (Bergelson, 2003, pp. 394–395). In fact, unlike the United States, the European Union has specifically recognized, in principle and in discussion, the differences in privacy claims against the government and private individuals, and in establishing the fundamental framework for the consent of sharing PII (Litan & Swire, 1998, p. 683). The United States continues to prefer a voluntary, self-regulatory approach to data privacy protections, and has established the Safe Harbor framework to facilitate international business operations for U.S. companies dealing with personal data (Export.gov., 2012). While the United States shares democratic principles with EU member states, as of now, U.S. citizens do not share in similar privacy protections.

C. PRIVACY PROTECTIONS ABROAD

While the U.S. courts grapple with defining proper use of technology by government through facts specific to individual cases, the lack of data privacy protection for Americans is starting to have disparate impact in comparison to citizens of other countries. For example, Path, a social network company, uploaded the personal address book data to facilitate further data mining from over 2 million users without disclosure (Shih, 2012). While such action potentially places Path in violation of Britain's Data Privacy Act, Path users in the United States have no similar legal protections as no federal law protects the privacy rights of U.S. citizens against such actions and Fourth

Amendment limitations do not apply to private entities (Shih, 2012). Further, unlike the United States where PII may be stored for subsequent use with minimal legal restriction, within much of the European Union, such information must be destroyed pursuant to law as soon as it is no longer needed to conclude the transaction between the provider and consumer (Bignami, 2007, p. 238).

Many European countries offer specific enumerated privacy protections for their citizens. Within the European Union, data protection is treated as a basic human right (Bignami, 2007, p. 233). Countries that recognize explicit constitutional privacy protections for either the individual and/or the home include Belgium, Brazil, Finland, Greece, Israel, Italy, Spain, and Sweden (Privacy International, 2007). Some countries, like The Netherlands, grant specific rights of privacy to individual and, distinctly, to the home (The Netherlands Constitution).

Proportionality is a recurring theme under European privacy. Generally, the focus of European privacy laws is on maintaining the contextual integrity of individual privacy in light of governmental need for surveillance (Taylor, 2011, p. 460). For example, individual privacy protections under the German Constitution provide for proportionality in conducting governmental surveillance, with a preference for as minimal interference as possible with those subjected to surveillance (Zoufal, 2008, p. 138). In regards to data retention, the German constitutional requirement is four pronged, and requires 1) proportional data security standards, 2) proportional purpose limitation, 3) transparency, and, 4) judicial control and limitation (Bellanova, De Hert, & de Vries, 2010, p. 4).

The European focus on proportionality and balance in determining privacy interests is reflected within U.S. law, but is not as overt nor as strongly represented within U.S. statutory language, at least on a comprehensive level. For example, the standards for the Title III wiretap mandate balancing individual privacy and government interests by requiring that prior to the issue of a judicial order, other traditional, less invasive investigative means must have been addressed, as well as limits on the duration for a wiretap to ensure that the wiretap does not continue any longer than is necessary to achieve the objective of the authorization (18 U.S.C.A. § 2518(1) & (5)). The U.S. Constitution provides inherent rights, including the right to be free from unreasonable

search and seizure pursuant to the Fourth Amendment. However, constitutional law is one of interpretation, and the inclusion of technology into the fact pattern provides for differing outcomes as to what the constitutional protections actually mean. See, *Katz*, wherein the Court identifies the need for neutral predetermination of the scope of a search to protect against the government's sole discretion (*Katz v. United States*, pp. 358–359). Further, *Katz* also stands for the need to balance the individual's expectation of privacy, the subjective expectation, against that which society is willing to recognize as reasonable, the objective (pp. 360–361). As such, albeit within a less overt legal schematic, both the U.S. courts and Congress have recognized the need to balance governmental investigative need with individual privacy, in alignment with general EU concepts on privacy requiring proportionality in light of government electronic surveillance.

1. European Convention on Human Rights

The European Convention of Human Rights (ECHR)[57] recognizes specific grants of privacy as a matter of inherent human right (Council of Europe, n.d.). The Council of Europe has treaty oversight for the ECHR, and both treaty and case law establish that ECHR rights are guaranteed to citizens within the European Union (Bignami, 2007, p. 241). Article 8 of the ECHR guarantees the right to private life and family life, but it also provides for restrictions of this right under certain circumstances (Morariu, 2009, p. 47). Article 8 protections are limited, and can be modified to safeguard national security, defense, public security, or the prevention, investigation, detection, and prosecution of criminal offenses (ECHR Article 8(2)). In Article 8, protections are subject to "public security" restrictions, the protections are fluid, and dependent upon the definitions existing within society at the time of definition (Morariu, 2009, p. 47).

As the ECHR relates to PII privacy, three principles emerge: 1) data collection and use must be conducted by a public authority for a public purpose, 2) the purpose must be legitimated, as defined in Article 8(2), and 3) the interference must be

[57] The Council of Europe includes 47 member countries and seeks to develop common principles based on the ECHR in the protection of individuals (Council of Europe, n.d.).

proportional in that it is the least burdensome intrusion in support of the public purpose (Bignami, 2007, p. 242). With regards to governmental surveillance, the ECHR language and interpretation supports the principle that regulation is necessary when interference with private life occurs due to governmental surveillance (Taylor, 2011, p. 461). The ECHR legal framework not only specifically delineates proper action; it inserts a requirement of governmental balance of need and proportionality. Despite judicial practice of balancing the private and governmental interests under Constitutional privacy review, other than the provisions of Title III wiretap requirements, the statutory address of privacy in the United States often lacks such balancing requirements.

2. Data Protection Acts

Data protection acts regulate the retention and use of derivative data rather than uses of a specific technology. As such, data protection laws are seen as technology neutral (Elaluf et al., 2011, p. 6). Unlike a Fourth Amendment review, which must first identify whether a protected privacy interest does exist, a data protection act defines the privacy interests protected and the applicable legal standards. Therefore, the law becomes a means to protect privacy by identifying when the privacy interest is substantial enough to demand state action rather than state neutrality (Taylor, 2011, p. 457). Given the growth and magnitude of pervasive, mass surveillance technology in use by both private and governmental actors, protection of PII is a growing concern. Data protection acts establish clear guidance for lawful action in regards to privacy standards regardless of the technology involved.

3. The European Union Data Retention Directive

Within the European Union, PII for citizens of member states is protected under The Data Retention Directive, (The Directive) (Council Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006).[58] The Directive provides guidance and standards for the collection and transmission of PII and other electronic data (Article 4 and Article 5). The Directive addresses data issues, such as the source and

[58] The Directive, Council Directive 2006/24/EC, 2006 O.J. (L 105) 54, is available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML.

destination of the communication, type and duration of the data, the type of equipment used, and the location and the identity of the party communicating (Morariu, 2009, p. 53). The Directive limits long-term access to PII by establishing retention limits of no less than six months and no greater than 24 months, absent certain exemptions (Article 6). Developed, in part, to address a perceived gap in PII access and use by law enforcement, The Directive exists to limit the amount of personal information available to the police (Bignami, 2007, p. 233). However, The Directive also allows for flexibility given that not all data is equal, and therefore, not equally protected (p. 236).

The Directive's call for proportionality arises out of ECHR Article 8(1), which grants respect for private and family life, home, and personal correspondence (ECHR Article 8(1)). However, the right to privacy is limited by the ECHR Article 8 exception of necessity (Article 8(2)). Necessity has been interpreted as requiring proportionality between the privacy interference and the pressing social need, for example, the protection of society from criminal activities (Morariu, 2009, pp. 54–55). As such, under the EU concept of proportionality a balancing of the individual's interests against those competing interests, usually those of government is required (Article 8(2)). Within this framework, The Directive serves to guide data privacy boundaries for its member nations in determining the proper proportion and balance of privacy interests.

EU member states still interpret and define the parameters of privacy within the laws of their individual nations. However, The Directive has certain standards, including adherence to the principal of proportionality, which requires determination as to whether the government's interference with the individual privacy right is commensurate in achieving the legitimate object that the state sought to achieve (Taylor, 2011, p. 461). Despite mandated implementation of The Directive for EU member countries, many countries have yet to implement fully the provisions of The Directive, particularly as it applies to the telecom and internet industries (Ringland, 2009). Individual EU states are left to interpret The Directive's provisions within the context of local law and standards.

4. A Practical Example—The United Kingdom

The United Kingdom and its experience with CCTV serves an example of the balancing of privacy interests within the EU system of law, ECHR Article 8 minimum privacy requirements, and PII data standards (Taylor, 2011, p. 467). The United Kingdom has engaged in the balancing of privacy and the government's use of surveillance technology since the early 1990s, when its early implementation of CCTV began with minimal regulation or oversight (Zoufal, 2008, p. 129).

Co-regulation, self-regulation with government, and private sector involvement, was a driver in the development of privacy standards for the U.K.'s early use of CCTV (Zoufal, 2008, p. 129). In part, the lack of formal legislation governing the use of surveillance technology contributed to the development of voluntary codes of practice and emerging standards for CCTV implementation (Webster, 2004, pp. 231–232). In effect, practice drove policy. However, as the use of CCTV surveillance grew, so did concerns over privacy. Given that the voluntary codes of practice did not have legal consequence, minimal relief or consequence for the failure to follow or enact standards to ensure privacy occurred.

a. Code of Practice

No statutory governance over CCTV surveillance of public areas occurred until March 1, 2000 when the U.K.'s Data Protection Act of 1998, (DPA), came into force (Information Commissioner, 2000, p. 2). The 2000 Code of Practice (2000 Code) incorporated the DPA's data protection principles while advocating for good practices and standardization of the use of CCTV (p. 2). The 2000 Code incorporated DPA mandates, including the criminalization of the use of an unregistered CCTV system to record people in a public or private place unless it meets certain criteria (The Data Protection Act of 1998, n.d.). The 2000 Code demonstrated an evolution of both thought and technology and included specific, articulated decision points as to whether the stated need for CCTV technology was proper and proportionate in relation to its use (Information Commissioner, 2000, pp. 6–7). By incorporating the DPA's legal

requirements with recommendations for best practices, the U.K. government sought to inform practice while striving for the accountability in the use of surveillance technology for both private and governmental entities.

Reflecting not only the changes in technology, but also those within society, the 2000 Code was updated in 2008 (Information Commissioner, 2008, p. 3). The 2008 Code was developed, in part, with the input of practitioners and had a goal of establishing more privacy oriented ways of using CCTV (p. 3). The 2008 Code updates were all based on the legally enforceable data protection principles of the 1998 Data Protection Act (p. 4). Unlike the earlier 2000 Code, the failure to adhere to the guidance within the 2008 Code could lead to legal consequence, with 62 legally enforceable standards to ensure compliance with the DPA (The Data Protection Act of 1998, n.d.). Further, the 2008 Code also included are 30 points of good practice, which together with the standards, were designed to build and maintain public confidence in CCTV systems and to ensure that they operate within the law (The Data Protection Act of 1998, n.d.). While the DPA mandated legal compliance, the recommendations for good practice sought to ensure that policy ensured privacy protections through actual practice.

Perhaps as a manifestation of the rapid development in technology and its use, only three years later in February 2011, the U.K. government sought formal guidance on updates to the 2008 Code. The consultation had the stated goal of ensuring the use of CCTV technology to promote public safety, while providing assurance that its use is reasonable, justifiable, and transparent (Home Office, 2011, p. 3).[59] This code update was expanded to include not only CCTV, but ANPR as well (p. 3). The progression of CCTV guidance from voluntary standards to those with measurable accountability and linked to a legally enforceable national data protection act demonstrates a public/private partnership centered on self-governing standards coupled with regulation that enhance privacy principles. Even absent formal legal action within the United States, the U.K. good practices model provides a policy option to develop consistent practice on surveillance technology.

[59] The consultation for input closed as of May 25, 2011. New publication has not yet occurred (Home Office, 2011).

b. U.K. Data Protection Challenge

The U.K.'s Code of Practice is linked to data protection, in that CCTV surveillance, as with most sensor surveillance technology, collects and stores PII (Taylor, 2002, p. 72). Both the DPA and the EU's governing standards have privacy protections for the individual. Within the United Kingdom, the individual's right to privacy exists not only in the initial collection of the PII data, but also in the subsequent dissemination of the data captured (Taylor, 2002, pp. 76–78). The review of the collection and use of surveillance data, as balanced against proportionality, arose in an early case before the Court on Human Rights.

In *Peck v. The U.K.*, the Court on Human Rights, (Strasbourg), accepted jurisdiction over a claim by a U.K. citizen, Geoffrey Peck, that the dissemination of CCTV footage of his public suicide attempt was an impermissible intrusion into his private life (*Case of Peck v. United Kingdom*, pp. 10–15). The Strasbourg Court found the release of the footage, which showed his actions upon the public way, to be a serious interference with the applicant's right to respect for his private life (p. 63).

In deciding the case, the court was tasked with balancing the interference with the private life of the individual against the public policy goals of CCTV, which sought to garner public confidence in CCTV through covert display of its ability maintain public order (*Case of Peck v. United Kingdom*, p. 79). The collection of the image, the actual suicide attempt, was not at issue for Mr. Peck, and the Court did not find issue with the initial collection (pp. 54, 60). The Strasbourg Court did focus on the broad dissemination of the CCTV surveillance, identified a potential pool of hundreds of thousands of viewers, and found that it created a serious interference with Mr. Peck's personal life (pp. 62–63). The Court held that while the government maintained a laudable policy goal of public safety and demonstrating the efficacy of CCTV, other options were available to protect the individual's privacy, inclusive of consent or masking of the individual, and found that the disclosure constituted a disproportionate, and therefore, unjustified interference with his private life, in violation of Article 8 of the Convention (pp. 80–87).

The *Peck* court's decision was based on the principles of proportionality in balancing the government's interest in the initial intrusion, the collection of the CCTV images in furtherance of public policy goals, against the available options for minimization of the privacy intrusion, the subsequent dissemination (*Case of Peck v. United Kingdom*, pp. 80–87). As the United Kingdom moves forward in its integration of CCTV and other pervasive mass surveillance technology, such as ANPR, within its Code of Practice, sensitivity to the subsequent retention and dissemination of the data calls for articulated policy and guiding standards. Data retention and collection becomes entwined with the general concepts of privacy intrusion as the data becomes more digitized, and therefore, accessible more broadly.

c. Statutory Data Protection within the United Kingdom.

Statutory privacy protections within the United Kingdom include the Data Protection Act(Data Protection Act 1998 c. 29). The domestic statutory protections are also supported through the ECHR and The Directive. Within the DPA, specific guidance exists for the legal processing of PII data, as well as the retention and publication of such data. Section 20 requires notice for the collection of PII, and Section 21 makes it an offense for failure to notify, absent due diligence. Article 55 identifies the penalties for violations of the DPA. Part VI of the DPA identifies the authority and scope of the information ministers duties (See Articles 51–54). The DPA readily and clearly identifies the administrative guidelines for collection and dissemination of PII.

Unlike the United States, where no single agency has responsibility for the oversight of privacy information, the DPA establishes an Information Commissioner, with not only the responsibility for oversight, but whose duties include developing Codes of Practice (Article 52). Any entity, public or private, engaged in processing PII data must register with the Commissioner (Information Commissioner's Office, n.d.). As such, the complex issue of proportionality in the use and retention of PII becomes more standardized, given a central decision point, and oversight and published regulations and codes of practice, within the United Kingdom, as compared to the United States.

For data protection laws to have value, they must be effective. Regardless of the written word, data protection rights, in and of themselves, must be supported by policy and standards to guide government activity in regards to surveillance, both overt and covert (Taylor, 2011, p. 467). From a government perspective, protecting privacy should not merely be about ensuring compliance with the requirements of a specific law, but rather incorporating principles of human rights as a commonsense, ethical requirement in the conduct of surveillance (National Research Council of the National Academie, 2008, p. 53). Yet, civil libertarians are ambivalent about the existence of data protection acts, as support may be seen as acquiescence to the prevalence of surveillance as the norm, rather than mass surveillance generating a privacy concern in and of itself (Morariu, 2009, p. 58). However, the gate is open, so to speak, and no privacy value derives from ignoring the growing web of governmental and private mass surveillance in U.S. society.

Regulation and accountability for collection and use of PII would serve to further individual privacy interests. Given the private data disclosed when engaging in a variety of daily activities, acceptance of surveillance in U.S. society, be it from government or private entities, may become the norm (*United States v. Jones*, p. 962). The U.K. CCTV Code of Practice demonstrates how government can facilitate public awareness, open discussion, and collaboration on the issue of privacy, data protection, public safety, and government accountability. Minimally, a similar call for an initial guidance review of existing practices within the United States might provide for a better informed public discussion on the status of the use of sensor technology for mass surveillance.[60]

[60] Recently, the White House published a document on consumer privacy, which set forth a call to action for the various stakeholders involved in protecting consumer privacy in a networked world, under the guidance of the Federal Trade Commission, to develop a statement of basic privacy principles and a sustained commitment by all stakeholders to address consumer privacy issues. Therefore, such a call to action for surveillance technology is not necessarily without foundation (Consumer Data Privacy in a Networked World, 2012).

THIS PAGE INTENTIONALLY LEFT BLANK

V. POLICY OPTIONS FOR MASS SURVEILLANCE

> New surveillance systems will fundamentally alter the relationship between government and citizens.
>
> –Justice Sotomayor

Several options are presented below that would provide options to bridge the gap and serve to protect privacy rather than merely limit the use of a specific technology. However, ensuring the proper balance between privacy and public safety is more a matter of subjective balancing rather than science. A variety of options exist to address the growing challenge of maintaining privacy given the expansive of pervasive mass surveillance, but none are all encompassing. The options explored include 1) self-governance over the use of sensor technology, 2) use of the judicial process to continue to define the limits of the government's use of surveillance technology under existing Fourth Amendment doctrine, 3) state control and definition of the privacy protections afforded their citizens, or 4) enacting comprehensive federal legislation to address the government's use of sensor technology and the derivative PII data that results. Of these four options, the first has negligible accountability for those establishing self-governed standards. The second and third options represent the status quo and provide no additional safeguards for civil liberties and minimal direction for law enforcement in the furtherance of privacy protections. The fourth option, while providing long-term protection for privacy, requires political will to address an increasingly complex legal and social problem arising out of the mass surveillance of the movement by citizens in public by government. No single option is a panacea for protecting privacy, but ignoring the growing web of surveillance, and collection and dissemination of PII serves neither privacy interests nor government's public safety needs.

A. SELF-GOVERNING STANDARDS

Establishing self-governing standards demonstrates commitment to civil liberties and legal mass surveillance practices. Further, voluntary, self-imposed standards provide for self-determination over mass surveillance policies and practices in light of legal

inertia. However, from a civil liberties perspective, self-governing standards are less than satisfactory in that they often lack outside review oversight and transparency and are malleable. One area in which self-regulation has been relatively successful is for newly developing technology, where economic issues exist in addition to privacy issues. For example, with Near Field Communications,[61] the European Union encouraged self-regulation to facilitate open competition and quick development of economically sustainable business models using the technology (Elaluf et al., 2011, p. 46). Also, within the United Kingdom, given the lack of formal regulation standards, co-regulation, a similar process to self-regulation, occurred with the initial development of CCTV (Zoufal, 2008, p. 129). However, as demonstrated by the updates in the U.K.'s Code of Practice and the ensuing increase in legal oversight of CCTV, privacy standards evolve with the technology and its acceptance within society. It may well be that self-regulation works better in the early stages of surveillance technology implementation, while the parameters of use are rapidly evolving and the full extent of the beneficial use of the technology, as well as its privacy implications, remains unknown. Within the United States, the need for caution in establishing legal parameters ahead of the social acceptance and use of technology with society has been voiced by the Supreme Court (*City of Ontario v. Quon*, p. 2,629).

Within the United States, self-regulation around surveillance technology has mostly developed through so-called model policies, which lack legal authority for mandated implementation or oversight. For example, The Constitution Project[62] has published "Guidelines for Public Surveillance" with policy recommendations for law enforcement's use of surveillance technologies (Constitution Project, 2007). Professional groups, such as the IACP, which is comprised of criminal justice stakeholders, also draft model policy recommendations for its members, including the "Privacy Impact Assessment Report for the Utilization of Automated License Plate Readers" (IACP,

[61] Near Field Communication enhances RFID systems by allowing two-way communication between endpoints, smart phones or other enabled devices. As compared to earlier RFID systems that were one-way only, two-way communication between enabled devices allows payment contacts or other such actions (Nosowitz, 2011).

[62] The Constitution Project is a bipartisan group focused on providing credible policy recommendations for a myriad of challenging constitutional.

2009). However, these types of policy recommendations are often generalized given the wide variance in statutory regulation and organizational structures among the states. Therefore, it is up to the individual members to determine whether the recommendations are legally appropriate for their jurisdiction and, if so, whether they will adopt or adapt the policy recommendations.

Additionally, many governmental agencies, inclusive of public safety agencies, draft internal policies governing the use of surveillance technology. Voluntary adoption of privacy policies can be a concrete representation of an agency's commitment to ensuring appropriate standards are in place to protect civil liberties. The DHS Traveler Redress Inquiry Program, (DHS TRIP), is one example of voluntary standards. Policies and procedures for individuals regarding restrictions on flight and their ability to petition the DHS TSA should they believe that government has incorrect information regarding their status are available publicly through the DHS website, thereby enhancing transparency and accountability for the organization's now public standards.[63] Law enforcement agencies also adopt procedures relative to surveillance and other privacy policies, which facilitate accountability and transparency (General Order 03-05 Video Surveillance Technology, 2011).

However, internally drafted policies are malleable, as they are subject to modification based upon executive decision, and as a result, often lack the gravitas of legal mandate. Additionally, no legal means exists to guarantee the adoption of or adherence to voluntary, self-initiated standards. The failure of mandated adherence becomes an issue for private entities where economics and not social policy drive decisions. Therefore, self-regulation is not always embraced as an effective solution, particularly in the arena of privacy and civil liberty protections. Yet, in the absence of specific legal guidance, self-regulation over the use of surveillance technology and policy provides for autonomy and can be used to address the gap between public concern and government accountability.

[63] The DHS TRIP program (Homeland Security, n.d.a.).

B. JUDICIAL DECISION PROCESS

The Fourth Amendment has traditionally been used to define the legal parameters for allowable governmental intrusion into the private lives of its citizens. A line of Supreme Court decisions, dating back to the 1928 decision in *Olmstead v. United States* and continuing through the Supreme Court's 2012 decision in *United States v. Jones*, have attempted to define the limitations on government's intrusion into the private realm of its citizens through the use of technology. However, Fourth Amendment judicial doctrine for developing technologies favors judicial caution with deference to legislative action relative to rules involving law enforcement investigations (Kerr, 2004, p. 805). Whether the precedent driven legal process of the U.S. courts remains a viable method for addressing privacy concerns in a digital age is still under debate.

While technology advances rapidly, the legal decision process under the Fourth Amendment is incremental. Further, because judicial review under the Fourth Amendment is factually driven, the decisions are often seen as inconsistent, even when based upon seemingly similar technologies (Capper, 2011, p. 191). In 1928, the technology driving the privacy concerns before the court was the government's use of a wiretap to eavesdrop on phone calls originating within the home (*Olmstead v. United States*). The *Olmstead* Court held that no Fourth Amendment search occurred absent a physical intrusion by the government (p. 438). Almost 40 years later, the U.S. Supreme Court reviewed a privacy claim involving the same technology but a different location—a public phone booth. In 1967, the Supreme Court decided *Katz v. United States*, holding that the Fourth Amendment protects people and not places (*Katz v. United States*, p. 351). Retreating from *Olmstead*, the *Katz* court ruled that a reasonable expectation of privacy, protected under the Fourth Amendment, might exist independent of the location of intrusion, be it in the home or in public (*Katz v. United States*, p. 353).

Subsequently, new technologies continue to come before the U.S. Supreme Court; however, rather than address the privacy impact, the Supreme Court continues to review how technology is used, under a framework established using landline telephones. Beeper tracking technology, thermal infrared surveillance, and GPS, have all been decided in the ensuing years, all under the precedence of the *Katz* standard of reasonable expectation of

privacy (*United States v. Knotts*; *United States v. Karo*; *Kyllo v. United States*; *United States v. Jones*). Lower courts are deciding cases involving GPS and cellular telephone tracking (*United States v. Bermudez*; *United States v. Amaral-Estrada*; *United States v. Flores-Lopez In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to Government*). However, reluctance continues to occur in reviewing these technologies anew by deciding upon the privacy impact of new, more intrusive technology rather than the government's use of the technology. As a result, modern surveillance technology and its resulting digital lode of PII is reviewed within a legal framework established over 55 years ago when the technology in issue was eavesdropping on a landline telephone.

Courts seek to narrow the issues under decision, thereby neglecting complexity, which is a hazardous way to set public policy on privacy and technology (Hosein, 2010, p. 153). The Supreme Court's decision in *Jones*, which ignored the issues raised by pervasive mass surveillance by government, provides a concrete example of the ability to narrow an issue to avoid complexity. As a result, judicially driven law on mass surveillance technology may not provide adequate guidance for government nor serve to protect individual privacy.

Further, judicial determinations, based on specific facts, before the courts drive case law, and the resulting distinctions based upon those facts, often fail to provide for clear guidance for the government's use of surveillance technology. With technology, the application of past facts to determine current legal outcomes may well be comparing apples to oranges. The Supreme Court has recognized that rapid changes in the dynamics of communication are not just evident in the technology, but also in what society accepts as proper behavior (*City of Ontario v. Quon*, p. 2623). The judicial case law process, with its focus on established precedent, is faulty from the start if the technologies that guided the precedent bear no resemblance to those currently under review (Herbert, 2011, pp. 448–450).

Additionally, as newer technology emerges, the level and degree of the government's physical intrusion into personal space, a touchstone of Fourth Amendment analysis, becomes less identifiable. Physical privacy intrusions, as opposed to pervasive

government surveillance, resonate more readily within the public psyche, as evidenced by the ongoing public outrage and governmental adjustment resulting from the very public inconvenience and indignity of airport screening (Harris, 2012). However, modern surveillance technology can be far more intrusive and far less visible than traditional physical searches. For example, the pinging of cell phones through cellular tower triangulation does not technically intrude upon an individual's personal space, but does provide information not only about movement across public space, but allows for continual surveillance of the individual's every movement, which in turn, provides significant PII regarding the person carrying the cellular phone being tracked (*United States v. Jones*, p. 933).

Despite years of recognition of the privacy impact that technology brings, the U.S. Supreme Court remains ambivalent in establishing Fourth Amendment standards that limit the government's use of mass surveillance technology. On the one hand, the Court has stated that the law must account for the advancement of technology and the implications for privacy as a result (*Kyllo v. United States*, p. 36). On the other hand, it has also noted that the use of technology in novel ways creates thorny problems and no need exists to rush to resolution if it is not necessary to address the privacy issue before the Court (*United States v. Jones*, p. 954). Despite a long history of raising concerns over the impact of technology and privacy, the U.S. Supreme Court continues to maintain that in 2012, it is still not the time to address the impact of technology and long-term surveillance (p. 954). The current Fourth Amendment framework, which requires independent analysis of each new technology through past legal precedence, serves neither the needs of the government in conducting criminal investigations nor the privacy protections sought by civil libertarians.

The U.S. Supreme Court's restraint, as evidenced in narrowly drawn decisions about how a technology is used by the government, despite decades of voicing concerns over the potential privacy impact of mass aggregation of data, fails to ensure timely address of constitutional privacy issues. However, modern life is intertwined with technology, which provides a data rich information environment in which absent legal restraint, government could readily obtain the intimate details of the daily lives of its

citizens with relative ease (Bignami, 2007, pp. 235–236). As a result, given its adherence to precedent, Fourth Amendment doctrine is often not as robust as is needed to address the rapidly evolving privacy issues surrounding the government's rapidly evolving use of mass surveillance technology and the subsequent privacy impact of its use, dissemination and retention of the data derived from these technologies.

C. LEGISLATIVE OPTIONS FOR PRIVACY PROTECTIONS

The Fourth Amendment has been the focus for privacy issues arising from criminal investigations using new technology; it is statutory law that generates real privacy protections (Kerr, 2004, p. 807). The legislative process is more nimble than the precedential driven judicial law process (Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council, 2008, pp. 152–153). Further, the courts have already demonstrated deference to Congress in regards to technology standards, as evidenced by the enactment and the court's adherence to Title III. Therefore, definitive legislative guidelines on privacy and data protection would inform and guide both citizens and government, while ensuring protection of civil liberties.

However, statutory protections for privacy are often issue specific, derived from a patchwork of federal and local laws (Stanley & Steinhardt, 2003, p. 15). Further, the varying judicial decisions that attempt to reconcile Fourth Amendment law with local and federal statutes that govern specific privacy interests create uncertainty as to privacy standards. In an age in which technology enhances the government's ability to mass monitor the public movement of its citizens, the absence of firm, guiding statutory privacy laws creates fissures for civil liberty protections and HLS.

1. State Oversight of Privacy Rights of its Citizens

The states are left to determine privacy standards as appropriate, absent federal law pre-emption or in light of an explicit grant of authority (Lane, 2003, p. 128). The Supreme Court has held that general rights of privacy are the responsibility of the states (*Katz v. United States*, pp. 350–351). Some states currently have explicit privacy protections for their residents. For example, the Florida Constitution provides that "Every

natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein (Florida State Constitution, art. 1, sec. 23). "A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way" (*United States v. Jones*, p. 934). In some respects, the states have stepped up to ensure privacy protections of their citizens in the absence of federal guidance.

Using GPS as an example, some states, including California, have statutorily limited the right to track a person electronically to law enforcement by identifying that using GPS without a person's knowledge is a violation of a reasonable expectation of privacy. See, e.g., California Penal Code section 637.7, Stats. 1998 c. 449(S.B.1667)§2. Other states, including those, such as Pennsylvania, South Carolina, Minnesota, and Florida, all legislatively address the standards for use of GPS by law enforcement, with some mandating law enforcement officers must obtain a warrant prior to use of GPS. See, e.g., 18 Pennsylvania Constitutional Statute § 5761; South Carolina Code Annotated § 17-30-140; Minnesota Statute § 626A.37, §626A.35; and Florida Statute § 934.06, 934.42). Seceding responsibility for statutory privacy to the states would generate 52 different sets of rules governing the conduct of governmental surveillance.

Additionally, state legislated privacy rights are limited protections in that they provide protections only within the state. Reconciling differing privacy standards under the laws of the individual states would be problematic for law enforcement and for individual privacy in an increasingly mobile world, as the type and degree of privacy protections would be based upon geography rather than standardized legal rule. Granting sole jurisdiction over privacy to the states may also negatively impact interstate criminal investigations, with state lines determining whether an investigation can continue and under what rules of engagement. Reserving the protection of privacy to the individual states, as called for in *Katz*, not only creates inconsistent privacy rights among U.S. citizens, it creates barriers for criminal investigations across state lines.

Examining privacy from a data collection and dissemination perspective, the outcome of mass surveillance by the government further compounds the problems arising from state legislative control of privacy. Within the realm of HLS, sharing information is

often a critical component of public safety strategies (Department of Homeland Security Information Sharing and Safeguarding Strategy, n.d.). Ostensibly, mass surveillance data is collected and retained to benefit public safety further. Therefore, surveillance is predicated upon the subsequent use and dissemination in the investigation of crime. However, if one state allows law enforcement to collect and store certain data, yet another prevents such collection, then significant practical and legal barriers arise. As a practical effect, the most restrictive state law becomes the controlling norm for any criminal investigation that might possibly cross-state borders, even if it does not. For example, within the Washington, DC area, four states converge within a relatively narrow geographic area. Would a law enforcement investigation risk the possibility of losing evidence of a crime if it occurs within one jurisdiction that does not have the same privacy standards as another? Finally, with today's surveillance technology, an individual does not have to be physically present to conduct surveillance or to collect PII data. Therefore, a state may not have legal jurisdiction over distance-based surveillance and data collection, another impediment to ensuring privacy[64] (Lane, 2003, p. 128).

States are stepping up to fill the privacy gap that affects their citizens in the absence of federal guidance for limitations on privacy intrusions. States are also establishing broader protections for their citizens, seemingly rejecting the confusing and restrictive interpretation of privacy under the Fourth Amendment (Gershman, 2010, p. 929). However, given the expanding use of technology, digital social networks, and the mobility of modern society, determination of privacy rights through land boundaries does not make practical sense—either for individual privacy or for law enforcement investigations. As such, the concept of the states as shepherds of individual privacy rights fails to protect individual privacy fully given the prevalence of mass surveillance and technology advancements.

[64] While not a subject of this thesis, in that much of electronic communication can be seen as a form of interstate commerce, the level and degree of protection that the states could provide for its citizens may be negatively impacted by federal laws, such as the Interstate Commerce Clause. For example, the web's underlying telecommunications infrastructure is already regulated through federal law.

2. Federal Legislative Prerogative

Congress successfully addressed privacy concerns raised through law enforcement's use of surveillance technology by establishing federal standards for eavesdropping under Title III. Effective measures to address the current legal and privacy concerns resulting from the government's use of mass surveillance technologies will require no less an exercise of legislative authority, particularly so given the variable and distinct legal mandates that currently address surveillance technology and other privacy interests. Additionally, the wide range of surveillance technologies currently in use will make individuated legislation challenging.

Existing federal legislation addresses privacy concerns arising from technology, albeit not on a coordinated, comprehensive scale. One example of such federal legislation is HIPAA, which was Congress' response to the explosive growth of technology in the medical field (EPIC, n.d.c.). Among other standards, HIPAA identifies who is covered, what information is covered, and its permitted uses and disclosures, as well as mandating the notice of privacy practices and establishing rights (U.S. Department of Health and Human Services, n.d.). Other federal privacy laws address some of the broader data collection and/or privacy protection issues, including the Electronic Privacy Communications (ECPA), the Privacy Act of 1974, or the E-Government Act of 2002. However, these laws are either issue specific or fail to address privacy protections comprehensively. For example, The Privacy Act and E-Government Act apply primarily to the federal government. ECPA is somewhat limiting in that it provides different protections based on where email is held and offers varying degrees of privacy based upon the perceived importance of the privacy interest involved (Justice Information Sharing, n.d.). Additionally, absent limited exceptions, federal legislation fails to provide comprehensive guidance or accountability for local law enforcement agencies that use surveillance technology.

Congress has legislative authority to enact privacy standards, and recently, an attempt was made to exert federal jurisdiction over surveillance standards for GPS through The GPS Act, which remains pending before Congress (GPS Act, n.d.). As Title III did for wiretapping, should The GPS Act pass, it will provide a comprehensive

statutory legislative framework for GPS surveillance (Wyden, n.d.). Statutory guidance for lawful GPS surveillance during criminal investigations would serve to assist law enforcement. Given the Supreme Court's decision in *Jone*s that avoided ruling on the privacy implications generated by the mass surveillance capacity of GPS, The GPS Act would define limitations for governmental action and provide explicit individual privacy protections that the courts are unwilling or unable to address. Another recent example of Congressional legislative action around privacy was the recent attempt to enact ECPA 2012 (H.R. 2471. (112th): Electronic Communications Privacy Act Amendments Act of 2012). In introducing the bill, Senator Leahy sought to update ECPA to keep pace with technology (Savage, 2012). One key provision is that the bill seeks to provide the same protections for emails stored by third parties, as with papers stored in the home (Savage, 2012). Additionally, absent certain exemptions, a warrant would be needed to access the emails stored by a third party service provider (H.R. 2471, p. 3, line 18–26).

The federal legislative approach to privacy is not without barriers. Both The GPS Act, and ECPA 2012, remain pending bills, highlighting a key limitation of the legislative approach to protecting privacy, the need to have the political will to ensure passage into law. Further, Congressional focus remains myopic and generally only addresses a single or limited privacy issue. As seen with HIPAA, The GPS Act, and ECPA 2012, the privacy concerns that drive the legislation, the impact of mass surveillance and data collection on the private lives of citizens, are recurrent, even if the technology is not. In this regard, Congress parallels the courts in addressing only the technology vehicle rather than the underlying civil liberty concern—privacy.

D. CONCLUSION

As technology changes, expectations of privacy may shift, but the underlying civil liberty protections for privacy should remain. Through its legislative authority, Congress is in the unique position of being able to protect individual privacy, rather than merely limiting how government uses a specific technology to conduct surveillance of its citizens. Proper balancing of individual privacy and governmental need requires Congress to establish the rules governing information gathering and for the courts to

evaluate those rules (Solove, 2010, p. 1538). Given the lengthy delay for legal decision and the law's inability to be sufficiently flexible to adapt to the rapidly evolving surveillance technology in use within the HLS field, a new approach is needed. Rather than having the courts continue to fail to bridge the growing gap between surveillance technology and individual privacy, Congress can step forward now to the protect the privacy of Americans from unwarranted intrusions from both governmental and private entities by enacting a federal data protection act.

Comprehensive statutory data privacy protection is needed because the existing patchwork of federal, state and local privacy laws are insufficient to address privacy in a digital age. Further, most privacy legislation is centered on a specific issue or technology, and therefore, does not address the government's expanding use mass surveillance technology to monitor the public movement of its citizens. Where national conformity is valued, federal law is the more useful vehicle to ensure consistency (Lane, 2003, p. 136). Exercise of federal jurisdiction over data privacy would ensure consistent, minimal standards for privacy protection with clear rules of engagement for all, including private entities. Given that PII and its use and retention, the byproduct of mass surveillance technology, is not specifically addressed in a structured, comprehensive law within the United States, a federal data privacy protection act would ensure privacy protections for U.S. citizens based upon identified privacy values rather than reactive legislation to address new technology developments.

No perfect balance exists for protecting civil liberties while supporting governmental surveillance in the furtherance of the investigation of criminal acts, inclusive of terrorism. The law, although jealous of individual privacy, has not kept pace with advances in technology (*Berger v. New York*, p. 48).[65] Eventually, precedential legal review centered on specific facts involving a specific technology will fail in providing any real privacy protections for U.S. citizens. While technology has changed the American way of life, when it comes to the delivery of privacy protections to U.S.

[65] While the *Berger* court grappled with landline telephones and older eavesdropping technology, the privacy concern over technology's rapid encroachment has remained voluble in the time since that decision.

citizens, the law relies upon a legal framework that evolves from the use of a landline telephone in a public telephone booth (*Katz v. United States*). At some point, the speed in which technology evolves will bypass precedential relevance, akin to comparing how to change the channels on a television; the remote is simply quite distinct and unique from manually changing a dial, and they do not compare.

Privacy determinations under the Fourth Amendment take years and the individual legal skirmish lines drawn with each new surveillance technology and its use create uncertainty. For example, over seven years had passed from the installation of the GPS device by the government to the Supreme Court's decision in *Jones* (*United States v. Jones*, p. 947); seven years of continued use and investment in GPS surveillance by the government and continued uncertainty as to the privacy implications of pervasive mass surveillance generated through the use of GPS. Given the Supreme Court's narrow decision in *Jones*, which relied upon trespass theory, the legal uncertainties still remain for "novel modes of surveillance," and are left for the lower courts to address (p. 954).

For every new surveillance technology used, law enforcement agencies are left to guess whether its use will comport with the eventual decision of the Supreme Court. Not only does this uncertainty generate social costs based upon civil liberties concerns, but the years of delay in arriving at final judicial decision generates significant financial costs given the actual dollars spent on technology investments and the potential for financial waste if a court subsequently determines that the use of a specific technology violates the Fourth Amendment. Further, Fourth Amendment doctrine has no legal authority over the growing private sector's use of sensor technology and the subsequent commodification of the derivative PII data. Alternatively, a federal data protection act would identify the privacy interests protected, rather than subsequently determining the limits for government actions in using a specific technology.

Technology will continue to move the social norms for the boundaries of individual privacy given its advancement and prevalence within U.S. society. The more the courts continue to voice concerns about technology's encroaching impact upon privacy, without action taken to limit that encroachment, the less likely it will be that privacy remains a viable legal concept. Further, the *Katz* two-pronged reasonable

expectation of privacy standard may well support judicial determinations that any mass surveillance technology used by government is not a search for Fourth Amendment purposes, given the pervasive presence of mass surveillance within U.S. society. In turn, such a decision could thereby eliminate the subjective, individual expectation of privacy as a matter of law (*United States v. Jones*; Chemerinsky, 2006, p. 950).

Additionally, Fourth Amendment doctrine establishes permissible boundaries for governmental surveillance that may not comport with what individuals would expect as reasonable, as illustrated by the case law on cellular telephones. Judicial determinations hold no expectation of privacy is anticipated for location data when carrying a cellular telephone *(United States v. Bermudez*; *United States v. Amaral-Estrada*; *United States v. Flores-Lopez*). Yet, in purchasing a cellular telephone, most people would reasonably expect that they are purchasing a communication device and not a tracking device. However, given GPS technology embedded in cellular telephones and cellular tower location technology, cellular telephone users also carry a tracking device with them for a good portion of their daily activities, into and including the home, one that government can access with relatively minimal standards (*United States v. Bermudez*; *United States v. Amaral-Estrada*; *United States v. Flores-Lopez*).

The *Jones* court identified that thorny and vexing issues are associated with determining the privacy impact of long-term surveillance of its citizens by the government (*United States v. Jones*, p. 954). However, if defining privacy interests and the government's proper use of evolving surveillance technology is not needed now, at a time when Americans are actively monitored by the government and other tracking technology while merely going about their daily business, when do Fourth Amendment privacy concerns become relevant and timely? Whether disparate, individual judicial decisions are the manner in which Americans should have their privacy protected is subject to debate and question. However, as a matter of ensuring the civil liberties that Americans have traditionally enjoyed, legislative action defining what privacy interests will be protected is a far more logical, efficient, and effective option for protecting privacy in a digital age.

The government's increasing reliance upon sensor technologies fuels civil liberties concerns as ever larger databases result from the data collected through the use of sensor and other technology (Stanley & Steinhardt, 2003, p. 15). As the data obtained from sensor technologies becomes more aggregated and increasingly more capable of individuation, the privacy issue is not limited to one of intrusion, but rather one of dissemination—which is not a Fourth Amendment issue. A lack of clear guidelines and accountability for data collection and retention practices can result in civil liberties violations and create mistrust in government (Taylor, 2002, p. 1). Governmental reticence in curtailing the disproportionate use of technology serves little social or legal value; as lack of governmental guidance will likely lead to further privacy litigation and erode real privacy protections in the wake of technological advances. The judicial focus on the government's use of a specific technology not only impedes proper government surveillance, it obfuscates the real issue—privacy.

Given the lethargy of the courts in addressing the impact of surveillance technology on privacy interests, legislatures have stepped up to fill the gap, albeit through a piecemeal approach. While some federal privacy protections exist against surveillance and access to PII, no comprehensive legislation addresses the privacy rights of U.S. citizens. The statutory patchwork of privacy laws at both the federal and local level are often directed towards specific, limited privacy interests and provide little guidance for appropriate government surveillance. More than 50 federal statutes address various aspects of digital security either directly or indirectly, but no overarching legislative privacy framework exists (Fischer, 2012, pp. 1–2). Further, while some state legislatures have stepped up to legislate privacy protections for their citizens, the variance in local laws results in disparity in privacy protections, thereby creating limitations for effective criminal investigations given the mobility of persons within U.S. society.

A clear and consistent legislative mandate as to what privacy interests are protected, the level of protection afforded, and the defined rules of engagement for governmental surveillance and the use of sensor technology, will address the growing concern over technology's impact on civil liberties. Legislative action will also support the public safety efforts of government through a provision of clear guidance for criminal

investigations and standards for processing the derivative data provided with sensor technologies. Given that no major legislation focused on technology and security has been enacted since 2002, and that ECPA, the governing federal statute on digital privacy, was enacted in 1986, the need to address privacy and technology legislatively is long past due (Fischer, 2012).

A federal data protection statute would provide the comprehensive privacy protection needed as a result of the expansive growth and use of sensor technology in U.S. society, by both governmental and private entities. Even where new legislation has been provided, such as with the ECPA 2012, or the GPS Act, the legislative focus remains narrow, as with email communication and the need for a warrant to read emails, as proposed for the ECPA 2012, or the regulation of the use of a specific surveillance technology, GPS, under the GPS Act. However, as with case law driven by precedence, chasing technology through legislation will ultimately fail to protect privacy, because the development and use cycle for technology evolves far more rapidly than legislative action. The GPS Act was first introduced in 2011 and the ECPA 2012 was introduced in September 2012, yet neither has advanced (Govtrack.us, 2012). Both are responses to significant technology advances occurring for years prior to the introduction of legislation, and technology will continue to advance while Congress debates the values of specific provisions of the legislation (Sledge, 2012).

A data protection act would direct the debate toward what privacy interests should be protected rather than what technology uses should be legislated. Minimally, as seen in the European Union, such legislation could govern the creation and access to PII, and mandate predicates, such as relevance to the governmental need, limitation of subsequent scope of use and purpose, and digital minimization and erasure once the PII data is no longer needed for the investigation (Bignami, 2007, p. 236). Enactment of a data protection act would also put the United States on the same privacy foundation as other democratic governments in Europe and ensure open access and participation in the global society in which all now live. Interoperability within the global economy requires mutual recognition of commercial data privacy, and while individual legislative schemes may differ, mutually recognized privacy protections are needed (Consumer Data Privacy in a

Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy 2012, pp. 31–33). Further, by recognizing standardized privacy principles through a data protection act, individual privacy rights become standardized, which in turn, provides guidance and direction for the courts and law enforcement as to what privacy interests are protected, rather than trying to direct the use of a given surveillance technology. Finally, in enacting a data protection act, the government will clearly establish the inherent privacy rights of U.S. citizens, rather than leaving it for the judiciary to decide as a matter of discrete, fact-driven judicial review. In other words, such legislative action would mandate governmental accountability to its citizens.

Ultimately, it is the role and responsibility of the government to act with transparency and accountability to the citizens its serves, as well as to act with legitimate authority in ensuring public security using mass surveillance technology. While much of the daily life is recorded through various surveillance mechanisms, private and governmental, control over an individual's PII should remain inviolate. Advancing technology and recent legal decisions do not support such a claim, and privacy erosions continue, albeit in a piece meal fashion. However, "privacy is not a discrete commodity, possessed absolutely or not at all" (*Smith v. Maryland*, p. 749). Privacy has been at the heart of U.S. democracy from its inception and remains an integral value of democratic government (Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy 2012 [Pres. Obama introduction], p. 3). In the ultra-connected world in which all live, federal legislation addressing privacy through a comprehensive data protection act will go a long way in minding the gap between privacy and surveillance technology.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Aerospace Corporation. (2005, April 29). *GPS primer*. Retrieved from http://www.aero.org/education/primers/gps/index.html

All State Insurance. (n.d.). *Drive wise.* Retrieved from http://www.allstateebrochure.com/drivewise/drivewise.pdf.

American Civil Liberties Union. (2009). *Who's spying in your neighborhood*? Retrieved from http://www.aclu.org/node/20415/

American Civil Liberties Union Fusion Center Update. (2008, July). Retrieved from http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf

Anagnostopoulos, C., Anagnostopoulos, I., Giannoulos, I., Kayafas, E., Kolias, V., & Loumos, V. (2010, June 23–35). *Integrating RFID on event-based hemispheric imaging for internet of things assistive applications. PETRA'10*. Samos, Greece. Retrieved from ACM DL Digital Library website: http://dl.acm.org/citation.cfm?doid=1839294.1839367.

Anderson, N. (2011, June). *Bipartisan bill would end government's warrantless GPS tracking*. Retrieved from arstechnica website: http://arstechnica.com/tech-policy/news/2011/06/bipartisan-bill-would-end-governments-warrantless-gps-tracking.ars

Bagley, A. W. (2011, January 27). Don't be evil: The fourth amendment in the age of Google, national security, and digital papers and effects. *ALB. L.J. SCI. & TECH. 21*(1), 153. Retrieved from http://www.albanylawjournal.org/articles/Bagely_3.pdf

Baker, S. A. (2010). *Skating on stilts*. Stanford, CA: Hoover Institution at Leland Stanford Junior University.

Barabasi, A.-L. (2003). *Linked*. London, England: Plume Strand.

Barber, G., Bunn, L., Eydt, B., Karygiann, T, & Phillips, T. (2007, April). *Guidelines for securing radio frequency identification systems*. NIST Special Publication 800-98. Retrieved from National Institute of Standards and Technology website: http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf

Barnett, J. (2010, December 22). Critical infrastructure protection month. FCC Official Blog [Web log post]. Retrieved from FCC website: http://www.fcc.gov/blog/critical-infrastructure-protection-month

Barrett, C. M. (2002, Spring). FBI internet surveillance: The need for a natural rights application of the fourth amendment to insure internet privacy. *Richmond Journal of Law & Technology*, *8*(3), 16. Retrieved from Richmond Journal of Law and Technology website: http://www.law.richmond.edu/jolt/v8i3/article16.html

Bellanova, R., De Hert, P., de Vries, K., & Gutwirth, S. (2010, May 18). *Proportionality overrides unlimited surveillance*. Retrieved from CEPS Liberty and Security in Europe website: http://www.ceps.eu/book/proportionality-overrides-unlimited-surveillance

Bellavita, C. (2008, June). What is homeland security? *Homeland Security Affairs*, *IV*(2), 1–30. Retrieved from The Journal of the Naval Postgraduate School Center for Homeland Defense and Security website: http://www.hsaj.org

Bergelson, V. (2003). *It's personal but is it mine? Toward property rights in personal information*. Rutgers University (Newark) Legal Working Paper Series. Retrieved from SelectedWorks website: http://works.bepress.com/vera_bergelson/2

Bickel, R. D., Brinkley, S., & White, W. (2003, Fall). Seeing past privacy: Will the development and application of CCTV and other video security technology compromise an essential constitutional right in a democracy, or will the courts strike a proper balance? *Stetson Law Review*, *33*, 299.

Bignami, F. E. (2007). *Privacy and law enforcement in the European Union: The data retention directive*. Paper 1602. Retrieved from Duke Law Faculty Scholarship repository website: http://scholarship.law.duke.edu/faculty_scholarship/1602

Bilton, R. (2009, May 22). Camera grid to log numbers. Retrieved from BBC News website: http://news.bbc.co.uk/go/pr/fr/-/2/hi/programmes/whos_watching_you/8064333.stm

Black's law dictionary. (1979). Saint Paul, MN: West Publishing.

Border security: DHS seeking unattended sensors technology for border surveillance. (2010, August 11). Retrieved from Homeland Security Newswire website: http://www.homelandsecuritynewswire.com/dhs-seeking-unattended-sensors-technology-border-surveillance

Borkowski, M. *Testimony before the United States house committee on homeland security, subcommittee on border and maritime security. After SBInet—The future of technology on the border.* (2011, March 15). Retrieved from Homeland Security website: http://www.dhs.gov/news/2011/03/15/written-testimony-cbp-house-homeland-security-subcommittee-border-and-maritime

Bowyer, K. W., Hollingsworth, K., & Flynn, P. J. (2007). *Image understanding for Iris biometrics: A survey*. Technical Report. Notre Dame, IN: University of Notre Dame, Department of Computer Science and Engineering.

Brandeis, L. D., & Warren, S. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193. Retrieved from MIT Computer Science and Artificial Intelligence Laboratory website: http://groups.csail.mit.edu/mac/classes /6.805/articles/privacy/Privacy_brand_warr2.html

Breier, M. (2011, May 2). *Spot a pot hole in Escondido? There's an app for that*. Retrieved from San Diego Union Tribune website: http://www.utsandiego.com/news/2011/may/02/spot-pothole-escondido-theres-app/

Brito, J. (2004). Relax don't do it: Why RFID privacy concerns are exaggerated and legislation is premature. *UCLA Journal of Law and Technology*, *8*(2), 1–42. Retrieved from http://www.lawtechjournal.com/articles /2004/05_041220_brito.pdf

Burstein, A. J. (2008). Amending the ECPA to enable a culture of cybersecurity research. *Harvard Journal of Law and Technology*, *22*, 167.

Cameron, A., Kolodinski, E., May, H., & Williams, N. (2008, May 5). *Measuring the effects of video surveillance on crime in Los Angeles*. Prepared for the California Research Bureau CR-08-007. Retrieved from the USC School of Policy, Planning, and Development website: http://www.library.ca.gov/crb/08/08-007.pdf

Capper, S. (2011). *United States v. Jones and the debate over warrantless GPS surveillance on vehicles*. 2 Ala. C.R. & C.L.L. Rev. 175.

Casanova, M., & Roberts, D. (2012, August). *Automated license plate recognition (ALPR) use by law enforcement: Policy and operational guide*. Retrieved from National Criminal Justice Reference Service website: https://www.ncjrs.gov/pdffiles1/nij/grants/239605.pdf

Chemerinsky, E. (2006, November 13). *Rediscovering Brandeis's right to privacy.* Retrieved from the Duke Law Scholarship Repository website: http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2494&context=faculty_scholarship&seiredir=1&referer=http%3A%2F%2Fwww.google.com%2Furl%3Fsa%3Dt%26source%3Dweb%26cd%3D10%26ved%3D0CGIQFjAJ%26url%3Dhttp%253A%252F%252Fscholarship.law.duke.edu%252Fcgi%252Fviewcontent.cgi%253Farticle%253D2494%2526context%253Dfaculty_scholarship%26rct%3Dj%26q%3Dbrandeis%2520the%2520right%2520to%2520privacy%26ei%3Df6WXTqOfCpLMsQKm_9z6DQ%26usg%3DAFQjCNG2NmcxnaqlFK0kMRBLGcpLI9tZcQ#search=%22brandeis%20right%20privacy%22

Chen, B. Y. (2010, October 11). *Apple registers trademark for 'There's an app for that.'* Retrieved from Wired website: http://www.wired.com/gadgetlab/2010/10/app-for-that

Cheverie, J. (n.d). Electronic communications privacy act modernization act of 2012. [Web log post]. Retrieved from Educause website: http://www.educause.edu /blogs/cheverij/electronic-communications-privacy-act-modernization-act-2012

Chicago's video surveillance cameras: A pervasive and unregulated threat to our privacy. (2011, February). Retrieved from American Civil Liberties Union Illinois website: http://il.aclu.org/site/DocServer/Surveillance_Camera_Report1.pdf?docID=3261

Clancy, T. K. (2012, July 2). United States v. Jones: Fourth amendment applicability in the 21st century. *Ohio State Journal of Criminal Law*, *10*(1). Retrieved from Social Science Research Network website: http://ssrn.com/abstract=2097811

Clark, J. E., Langer, J. V., & Powell, T. D. (2010, Spring). What GPS might have been—and what it could become. *Crosslink*, *11*(1), 7–77. Retrieved from Space Library website: http://www.space-library.com/Crosslink_V11N1_2010spring.pdf

Clark, M. W. (2007). Cell phones as tracking devices. *Val. U. L. Rev*. *41*(4), 1413–1480. Retrieved from Valparaiso University Law Review website: http://scholar.valpo.edu/vulr/vol41/iss4/2

Cloud, M. (2002). Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment, *Mississippi Law Journal, 72*, 5, 28.

Coaffee, J. (2004, February 24). Rings of steel, rings of concrete and rings of confidence: Designing out terrorism in Central London pre and post September 11th. *International Journal of Urban and Regional Research*, *28*, 201–211.

Coaffee, J. (2006). From counterterrorism to resilience. *The European Legacy*, *11*(4), 389–403.

Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council. (2008). *Protecting individual privacy in the struggle against terrorists: A framework for program assessment*. Retrieved from Epic.org website: http://epic.org/misc/nrc_rept_100708.pdf

Computer Crime and Intellectual Property Section (CCIPS). (2009, September). *Searching & seizing computers and obtaining electronic evidence in criminal investigations*. (3rd ed.). Retrieved from the United States Department of Justice website: http://www.cybercrime.gov/ssmanual/index.html

Computer Science and Telecommunications Board. (2007). *Engaging privacy and information technology in a digital age*.

Connecting the dots. Surveillance in our society. (n.d.). Retrieved from the American Civil Liberties Union of Northern California website: http://www.aclunc.org/issues/government_surveillance/connecting_the_dots..._surveillance_in_our_society.shtml

Constance, J. K. (1995). Comment: Automated fingerprint identification systems: Issues and options surrounding their use to prevent welfare fraud. *Albany Law Review, 59*, 399–422.

The Constitution Project. (2007). Retrieved from http://www.constitutionproject.org

The Constitution Project. (2011, September 21). *Liberty and security committee statement on location tracking.* Retrieved from http://www.constitutionproject.org/pdf/LocationTrackingReport.pdf

Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy. (2012). Retrieved from the White House website: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

Cornell University Law School. (2010, August 19). *Stare decisis*. Retrieved from http://www.law.cornell.edu/wex/stare_decisis

Council of Europe. (n.d.). Retrieved from http://www.coe.int

Crosslink magazine. (2010, Spring). *11*(1). Retrieved from http://www.aero.org/publications/crosslink/spring2010/index.html

Cybersecurity Act of 2012, (S. 3414).

Data Privacy & Integrity Advisory Committee. (2006, December). *The use of RFID for human identity verification*. Retrieved from U.S. Department of Homeland Security website: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

The Data Protection Act of 1998. (n.d.). Retrieved from the CCTV Advisory Service website: http://www.cctv-information.co.uk/i/Data_Protection_Act

DeCew, J. W. (1997). *In pursuit of privacy: Law, ethics and the rise of technology.* Ithaca, NY: Cornell University Press.

Dempsey, J. X. (1997). Communications privacy in the digital age: Revitalizing the federal wiretap laws to enhance privacy. *Albany Law Journal of Science & Technology, 8*(1). Retrieved from Center for Democracy and Technology website: http://www.cdt.org/publications/lawreview/1997albany.shtml

Dempsey, M. (2010). *Eyes of the Army. U.S. Army roadmap for unmanned aircraft systems 2010–2035*. Retrieved from www.army.mil/Rucker website: http://www-rucker.army.mil/usaace/uas/US%20Army%20UAS%20RoadMap%202010%202035.pdf

Department of Homeland Security. (2009, April 1). *Privacy impact assessment for the security and video quality for the public safety statement of requirements project.*

Department of Homeland Security. (2010, June). *Privacy impact assessments. The privacy office official guidance*. Retrieved from the MIT Computer Science and Artificial Intelligence Laboratory website: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Department of homeland security information sharing and safeguarding strategy. (n.d). Retrieved from Department of Homeland Security website: http://www.dhs.gov/information-sharing-and-safeguarding-strategy

Digital government: Building a 21st century platform to serve the American people. (n.d.). Retrieved from The White House website: http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html

Dwyer, A. M., La Vigne, N. G., Lowry, S. S., & Markman, J. M. (2011, September). *Using public surveillance systems for crime control and prevention: A practical guide for law enforcement and their municipal partners*. Washington, DC: Urban Institute.

E-Z Pass Group. (n.d.). *About E-zpass*. Retrieved from http://www.e-zpassiag.com/about-e-zpass/how-does-it-work

ECPA reform and the revolution in location based technologies and services: Hearing before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong., 2nd Sess., 17–30 (2010). Retrieved from http://judiciary.house.gov/hearings/printers/111th/ 111-109_57082.PDF

The Editorial Board. (2013, January 6). *Black boxes are in 96% of new cars*. Retrieved from the USA Today website: http://www.usatoday.com/story/opinion /2013/01/06/black-boxes-cars-edr/1566098/

Elaluf-Calderwood, S., Hosein, G., Karrberg, P., & Liebenau, J. (2011, October). Near field communications; privacy, regulation & business models. *London School of Economics and Political Science*. Retrieved from LSE Research Online website: http://eprints.lse.ac.uk/39076/1/LSE-White-Paper_-_Near-Field-Communications-Privacy-Regulation-Business-Models.pdf

Electronic Communications Privacy Act. (2011). Retrieved from Electronic Privacy Information Center website: http://epic.org/privacy/ecpa/default.html

Electronic Communications Privacy Act of 1986, (ECPA), (18 U.S.C. § 2510–2522, Pub. L .99–508.

Electronic Privacy Information Center (EPIC). (n.d.a.). *Electronic Communications Privacy Act (EPCA).* Retrieved from http://epic.org/privacy/ecpa/default.html

Electronic Privacy Information Center (EPIC). (n.d.b.). *History of national identification cards*. Retrieved from http://epic.org/privacy/id_cards/#hist

Electronic Privacy Information Center (EPIC). (n.d.c.). *Medical record privacy*. Retrieved from http://epic.org/privacy/medical/

Electronic Privacy Information Center (EPIC). (n.d.d.). *Radio frequency identification (RFID) systems*. Retrieved from http://epic.org/privacy/rfid/

Electronic Privacy Information Center (EPIC). (2008). *National ID and the real ID act*. Retrieved from http://epic.org/privacy/id_cards/#resources

Electronic Privacy Information Center (EPIC). (2011). *Video privacy protection act.* Retrieved from http://epic.org/privacy/vppa/

Emmet, C. United States v. Pineda-Moreno. (2011). *Tracking down individuals' reasonable expectation of privacy in the information age*, *41*(3). Retrieved from Golden Gate University Law Review website: http://digitalcommons.law.ggu.edu/ggulrev/vol41/iss3/3

Enhanced driver's licenses: What are they? (n.d.). Retrieved from Department of Homeland Security website: http://www.dhs.gov/files/crossingborders/gc_1197575704846.shtm

Evolution and development of police technology. (1998, July 1). Retrieved from Police Technology website: http://www.police-technology.net/id59.html

Export.gov. (2012). *Welcome to the U.S.-EU safe harbor*. Retrieved from http://export.gov/safeharbor/eu/eg_main_018365.asp

Fact sheet: Enhanced driver's license. (2007, December 5). Retrieved from Department of Homeland Security website: http://www.dhs.gov/xnews/releases/pr_1196872524298.shtm

Federal Bureau of Investigation. (n.d). *Integrated automated fingerprint system.* Retrieved from http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis

Ferraresi, M. *GPS system will make police officers jobs easier, safer*. (2005, October 7). Retrieved from azcentral.com website: http://www.azcentral.com /community/scottsdale/articles/1007sr-technology07Z8.html?&wired

Fischer, E. A. (2012, November 9). *Federal laws relating to cybersecurity. Discussion of proposed revisions* (Congressional Report No. R42114). Washington DC: Library of Congress Congressional Research Service. Retrieved from Open CRS website: http://www.emptywheel.net/wp-content/uploads/2012/11/Federal-Laws-Relating-to-Cybersecurity-Discussion-of-Proposed-Revisions.pdf

Fisher, B. A. J., & Fisher, D. (2004).*Techniques of crime scene investigation*. (7th ed.). CRC Press, Inc.

Freiwald, S. (2007). First principles of communications privacy. *Stanford Technology Law Review, 3*. Retrieved from Stanford Technology Law Review website: http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf

Freiwald, S. (2011). Cell phone location data and the fourth amendment: A question of law, not fact. *Maryland Law Review, 70*, 681.

Garfinkel, S. (2000). *Database nation: The death of privacy in the 21st century*. Beijing, Cambridge, O'Reilly Media Incorporated.

General order 03-05 video surveillance technology. (2011, April 14). Retrieved from Chicago Police Department website: http://directives.chicagopolice.org/directives/

Gershman, B. L. (2010). Privacy revisited: GPS tracking as search and seizure. *Pace Law Review, 30*(3), 927–964. Retrieved from http://digitalcommons.pace.edu/cgi /viewcontent.cgi?article=1636&context=lawfaculty

Gibbons, G. (2009, January/February). *Critical infrastructure: The United States and GPS*. Retrieved from Inside GNSS website: http://www.insidegnss.com/node/1121

Glover, R. G. (2007, Summer). Symposium on electronic privacy in the information age: A probable nightmare: Lifting the fog from the cellular surveillance statutory catastrophe. *Valparaiso University Law Review, 41*, 1543.

Government Accounting Office. (2011, November 4). *Arizona border surveillance technology. More information on plans and costs is needed before proceeding* (GAO-12-22). Retrieved from http://gao.gov/products/GAO-12-22

Govtrack.us. (2012). *H.R. 6529 (112th): ECPA 2.0 Act of 2012*. Retrieved from http://www.govtrack.us/congress/bills/112/hr6529#related

GPS Act. (n.d). Retrieved from Ron Wyden website: http://wyden.senate.gov /issues/legislation/details/?id=b29a3450-f722-4571-96f0-83c8ededc332#faqs

GPS Act. 112th Congress (2011–2012) S.1212 and H.R. 2168.

GPS.gov. (2011, June 6). *What is GPS?* Retrieved from http://www.gps.gov/systems/gps/

Gramm–Leach–Bliley Act (GLBA), 15 U.S.C. § 6801 *et seq*.

Grance, T., McCallister, E., & Scarfone, K. (2010, April). *Guide to protecting the confidentiality of personally identifying information (PII). Recommendations of the national institute of technology.* Special Publication 800-122. Retrieved from the National Institute of Standards and Technology website: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

Granick, J. (2011, June 21). *Proposed GPS act clarifies, improves location privacy*. Retrieved from The Stanford Law School Center for Internet and Society website: http://cyberlaw.stanford.edu/node/6686

Gross, S., & Inkley, T. (2000, October 5). *Electronic records, public disclosure and privacy*. Retrieved from Municipal Research and Services Center of Washington website: http://www.mrsc.org/Subjects/InfoServ/privacy.aspx#1

Guidelines for public video surveillance. (2007). Retrieved from The Constitution Project website: http://www.constitutionproject.org/pdf/54.pdf

Gutwirth, S. (2002). *Privacy and the information age*. Landham, MD: Rowman & Littlefield Publishing

H.R. 2471. (112th): Electronic communications privacy act amendments act of 2012, 112th Cong., 2011–2013. Text as of November 29, 2012 (Reported by Senate Committee) (2012). Retrieved from govtrack.us website: http://www.govtrack.us/congress/bills/112/hr2471/text

Hamilton, L. & Keane, T. *Ten years after 9/11: A report from the 9/11 Commission Chairmen, United States Senate,* 112th Cong., 1st Sess. (2011). Retrieved from Homeland Security Digital Library website: http://www.hsdl.org/?view&did=7719

Harris, S. (2012, August 22). *Giving in to the surveillance state*. Retrieved from New York Times website: http://www.nytimes.com/2012/08/23/opinion/whos-watching-the-nsa-watchers.html?_r=1&nl=todaysheadlines&emc =edit_th_20120823

Harwood, M. (2010, March 24). *Police must use license plate readers with good judgment*. Retrieved from Security Management website: http://www.securitymanagement.com/news/police-must-use-license-plate-readers-with-good-judgment-006889

Health Insurance Portability and Accountability Act of 1996, (HIPAA). Pub. L. No. 104-191, §§ Pub. L. No. 104-191, 110 Stat. 1936 (1996)).

Heffernan, W. C. (2001 Fall/2002 Winter). Fourth amendment privacy interests. *Journal of Criminal Law & Criminology, 92*(1), 1–36.

Helft, M., & Miller, C. C. (2011, January 9). *1986 privacy law is outrun by the web*. Retrieved from New York Times website: http://www.nytimes.com/2011/01/10/technology/10privacy.html?_r=1&hp

Henderson, S. E. (2011). The Timely demise of the fourth amendment third party doctrine. *Iowa Law Review Bulletin, 96,* 39–51.

Hendry, J. (2008). Contemporary comparative law: Between theory and practice: Review of Esin Örücü & David Nelken's comparative law: A handbook. *German Law Journal, 9*, 2253–2262. Retrieved from Germany Law Journal website: http://www.germanlawjournal.com/index.php?pageID=11&artID=1067

Herbert, I. (2011). Where we are with location tracking: A look at the current technology and the implications on fourth amendment jurisprudence, *Berkeley J. Crim. L. 16*(2), 448–450.

Highest performing fingerprints sensors for handsets, tablets and PCs. (n.d.). Retrieved from http://www.validityinc.com/technology.php

Hodges, K. (2007, June). Tracking "bad guys" legal considerations in the use of GPS. *FBI Law Enforcement Bulletin*, 25–32.

Home Office. (2011). *Consultation on a code of practice relating to surveillance cameras.* Retrieved from http://www.homeoffice.gov.uk/publications/consultations/cons-2011-cctv/code-surveillance-cameras?view=Binary

Homeland Security Presidential Directive 7. (2003, December 17).

Homeland Security. (n.d.a.). *DHS traveler redress inquiry program (DHS TRIP).* Retrieved from http://www.dhs.gov/files/programs/gc_1169676919316.shtm

Homeland Security. (n.d.b.). *Enhanced driver's licenses: What are they?* Retrieved from http://www.dhs.gov/enhanced-drivers-licenses-what-are-they

Hosein, I., & Whitley, E. A. (2010). *Global challenges for identity policies*. Basingstoke, UK: Palgrave Macmillan.

HR. 2471. (n.d.). Retrieved from Patrick Leahy website: http://www.leahy.senate.gov/imo/media/doc/Leahy-Substitute-to-HR2471.pdf

Hutchins, R. (2012, January 29). A step back for rights. Retrieved from Baltimore Sun website: http://www.baltimoresun.com/news/opinion/oped/bs-ed-scotus-gps-20120129,0,934859.story

Hutchins, R. M. (2007, December). *Tied up in Knotts?* GPS technology and the fourth amendment. *UCLA Law Review*, *55*, 409–465.

Hutchins, R. M. (2010, May). Essay: The anatomy of a search: Intrusiveness and the fourth amendment. *University of Richmond Law Review*, *44*, 1185–1190.

ICT Regulation Toolkit. (n.d.). *Section 4.4 data protection/privacy laws*. Retrieved from http://www.ictregulationtoolkit.org/en/section.2107.html

Information Commissioner. (2000, July). *CCTV code of practice*. Retrieved from South Eastern Education and Library Board website: http://www.seelb.org.uk/data_protection/PDFs/CCTV_Code_Of_Practice.pdf

Information Commissioner. (2008). *CCTV code of practice*. Retrieved from http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf

Information Commissioner's Office (ICO). (n.d.). *Register (notify) under the data protection act.* Retrieved from http://www.ico.gov.uk/for_organisations/data_protection/notification.aspx

Innovation & technology our approach. (n.d.). Retrieved from Transportation Security Administration website: http://www.tsa.gov/approach/tech/

Institute for Intergovernmental Research. (n.d.). *Criminal intelligence systems operating policies (28 CFR Part 23).* Retrieved from http://www.iir.com/(X(1)S(3quzulqkzwxp3eye0wsrsvry))/Justice_Training/28cfr/default.aspx

International Association of Chiefs of Police (IACP). (2005, Fall). *Law enforcement priorities for public safety. Identifying critical technology needs. Technology survey results.* Retrieved from http://www.theiacp.org/LinkClick.aspx?fileticket=76jsKsxCEB0%3d&tabid=392

International Association of Chiefs of Police (IACP). (2009, September). *Privacy impact assessment report for the utilization of automated license plate readers*.

International Committee on Global Satellite Systems. (2010). *United Nations office for outer space affairs. Current and planned global and regional navigation satellite systems and satellite-based augmentations systems*. Retrieved form http://www.oosa.unvienna.org/pdf/publications/icg_ebook.pdf

Introna, L. D., & Nissenbaum, H. (2009, April 8). *Facial recognition technology. A survey of policy and implementation issues*. Retrieved from New York University website: http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf

Jallad, T. N. (2010, Spring). Old answers to new questions: GPS surveillance and the unwarranted need for warrants. *North Carolina Journal of Law & Technology, 11*(2), 351.

Johnson, O'Ryan. (2011, July 21). *Lawyer: Cop scanner 'crosses line.'* Retrieved from Boston Herald News website: http://bostonherald.com/news_opinion /local_coverage/2011/07/lawyer_cop_scanner_%E2%80%98crosses_line%E2%80%99

Justice Information Sharing. (n.d.) *Privacy and civil liberties*. Retrieved from http://it.ojp.gov/156default.aspx?area=privacy&page=1287#fisma

Kallen, S. A. (2006). *At issue: Are privacy rights being violated*. Detroit: MI: Thompson Gale.

Kamin, S. (2004). The private is public: The relevance of private actors in defining the fourth amendment. *Boston College Law Review, 46*, 83.

Kerr, O. S. (2004, March). The fourth amendment and new technologies: Constitutional myths and the case for caution. *Michigan Law Review, 102*, 801.

Kerr, O. S. (2005, December). Searches and seizures in a digital world. *Harvard Law Review, 119*(2), 531.

Kerr, O. S. (2011, April 5). Applying the mosaic theory of the fourth amendment to disclosure of stored records. The volokh conspiracy. [Web log post]. Retrieved from http://volokh.com/2011/04/05/applying-the-mosaic-theory-of-the-fourth-amendment-to-disclosure-of-stored-records/

Kerrane, K. (2011, March). A. Note: Keeping up with officer Jones: A comprehensive look at the fourth amendment and GPS surveillance. *Fordham Law Review, 79*, 1695–1742.

Kirkpatrick, M. (2010, January 9). *Facebook's Zuckerberg says the age of privacy is over*. Retrieved from Read Write website: http://www.readwriteweb.com /archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php

Koppel, A. (2010, April). NOTE: Warranting a warrant: Fourth amendment concerns raised by law enforcement's warrantless use of GPS and cellular phone tracking. *Miami Law Review*, *64*, 1062–1083. Retrieved from Miami Law Review website: http://www.law.miami.edu/studentorg/miami_law_review/issue_archive/vol64no3.php?op=13

Landis, B. (2009, October 11). *Is EZ-Pass infringing on people's privacy*? Retrieved from Providence Journal website: http://www.projo.com/news/content/NEW_TOLL_PRIVACY_10-11-09_VNG11U8_v18.361aaed.html

Lane, T. A. (2003). Of hammers and saws: The toolbox of federalism and sources of law for the web, *New Mexico Law Review*, *33*, 115, 128.

Lau, D. J. (n.d.). *Automatic license plate recognition*. Retrieved from Police Technology website: http://www.police-technology.net/automatic_license_plate_recognition.html

Ledebur, L. E. (2009). Plurality rule: Concurring opinions and a divided supreme court. *Penn State Law Review*, *113*, 899.

Legal Information Institute. (2010, August 19). *Stare decisis.* Retrieved from Cornell University Law School website: http://www.law.cornell.edu/wex/stare_decisis.

Levenson, L. L. (2011, June 6). *Do GPS tracking devices violate the fourth amendment*? Retrieved from the National Law Journal website: http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202496096259&slreturn=1&hbxlogin=1

Lichtblau, E. (2012a). *Cell carriers see rise in requests to aid surveillance.* Retrieved from New York Times website: http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=all

Lichtblau, E. (2012b). *Police are using phone surveillance as a routine tracking tool*. Retrieved from *New York Times* website: http://www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html?_r=1

Lipowicz, A. (2011, February 18). *CBP will begin new border protection strategy in Arizona*. Retrieved from GCN website: http://gcn.com/articles/2011/02/17/cbp-to-spend-750m-on-arizona-border-technologies.aspx

Litan, R., & Swire, P.P. (1998). *None of your business: world data flows, electronic commerce, and the European privacy directive*. Washington, DC: Brookings Institute Press.

Luna, E. G. (1999). Sovereignty and suspicion, *Duke Law Journal*, *48*, 787.

Malin, B., Newton, E., & Sweeney, L. (2003, March). *Preserving privacy by de-identifying facial images*. (master's thesis). Carnegie Mellon University, School of Computer Engineering. Retrieved from DTIC Online website: http://www.dtic.mil/cgi-bin/GetTRDoc?Location =U2&doc=GetTRDoc.pdf&AD=ADA460282

Manson, T. M. (2008, July). *License plate recognition*. Retrieved from Hendon Media Group website: http://www.hendonpub.com/resources/articlearchive /details.aspx?ID=206992

Marceau, J. F. (2011). The fourth amendment at a three-way stop. *Alabama Law Review*, *62*, 687–755.

Masiello, E. A. (2003). *Privacy implications of biometric surveillance: The destruction of anonymity*. (master's thesis). Wellesley College. Retrieved from betsym website: http://www.betsym.org/Privacy_Biometrics.pdf

McCallum, S. (n.d). *Evaulability assessment of mobile biometric facial recognition technology Pinellas County, Florida*. Retrieved from National Criminal Justice Reference Service website: https://www.ncjrs.gov/pdffiles1/nij/mobile-biometric-facial.pdf

McCarthy, T. J. (2008). *The rights of publicity and privacy*. § 5.59 (2nd ed.).

McCullagh, D. (2001, Fall). Technology as security. *Harvard Journal of Law & Public Policy*, *25*, 129–142.

McCullough, A. (2011, January 16). *Greenwood putting GPS into police cars*. Retrieved from Mississippi Business Journal website: http://msbusiness.com/2011/01/greenwood-putting-gps-in-police-cars/

Merriam Webster. (n.d.). *Privacy*. Retrieved from http://www.merriam-webster.com/dictionary/privacy?show=0&t=1318214829

Merrion, P. (2010, April 26). City pushes highway cams; Chasing fed funds for highway surveillance to Mexican border. *Crain's Business Daily*.

Meyers, J. (2011, June 11). *How to stop facebook's facial recognition software from automatically tagging you in photos*. Retrieved from Business Insider.com website: http://www.businessinsider.com/how-to-stop-facebooks-facial-recognition-software-from-automatically-tagging-you-in-photos-2011-6

Mitchell, J. (2011, June 30). Making tagging easier [Web log post]. Retrieved from http://blog.facebook.com/blog.php?post=467145887130

Moore, A. (2008, Fall). Defining privacy. *Journal of Social Philosophy*, *39*(3), 411–428. Retrieved from Wiley Online Library website: http://onlinelibrary.wiley.com/doi/10.1111/j.1467-9833.2008.00433.x/full

Moore, K. (2008, March 13). *Police cars will soon have GPS*. Retrieved from Daily Gazette.com website: http://www.dailygazette.com/news/2008/mar/13/0313_gpscity/

Morariu, M. (2009). How secure is to remain private? On the controversies of the European data retention directive. *Amsterdam Social Science*, *1*(2), 46–65. Retrieved from http://www.socialscience.nl/application/upload /files/vol1%20is2%20morariu.pdf

Moses, K. R. (2012). *The fingerprint source book. Chapter 6: Automated fingerprint identification system*. Retrieved from National Criminal Justice Reference Service website: https://www.ncjrs.gov/pdffiles1/nij/225326.pdf

Napolitano, J. (2009, April 21). *Border trade alliance international conference*. Retrieved from Department of Homeland Security website: http://www.dhs.gov/ynews/speeches/sp_1240361190144.shtm

National crime information center. (n.d). Retrieved from Federation of American Scientists website: http://www.fas.org/irp/agency/doj/fbi/is/ncic.htm

National Criminal Justice Reference Service. (1977, July). *Personal privacy in an information society*. Retrieved from website: http://www.ncjrs.gov/App/Publications/abstract.aspx?ID=49602

National Information Standards Organization (NISO). (2004). *Understanding metadata*. Retrieved from http://www.niso.org/publications/press/UnderstandingMetadata.pdf

National Institute of Justice. (2003, July). CCTV: Constant cameras track violators, *NIJ Journal*, *249*. Retrieved from National Criminal Justice Reference Service website: https://www.ncjrs.gov/pdffiles1/jr000249d.pdf

National Research Council of the National Academies. (2008). *Protecting individual privacy in the struggle against terrorists. A framework for program assessment*. Retrieved from the National Academy of Sciences website: http://www.nap.edu/openbook.php?record_id=12452&page=R2

National Science and Technology Council (NSTC). (2006, March 27). *Biometrics overview*. Retrieved from https://www.hsdl.org/?view&doc= 64466&coll=documents

The Netherlands Constitution. Article 10, Article 12, 1983.

New York State Department of Motor Vehicles. (n.d.). *Enhanced DMV photo documents for U.S. Citizens who are residents of NYS*. Retrieved from http://www.nydmv.state.ny.us/edl-main.htm

Newmarker, C. (2007, October 8). *E-ZPass records out cheaters in divorce court—gadgets*. Retrieved from MSNBC website: http://www.msnbc.msn.com/id/20216302/

Next generation identification. (n.d.). Retrieved from Federal Bureau of Investigation website: http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi

Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Journal of Law and Philosophy, 17*, 559–596. Retrieved from http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf

Nissenbaum, H. (2000, September 28). *The problem of privacy in public*. Retrieved from New York University website: http://www.nyu.edu/projects /nissenbaum/papers/privacy.pdf

Nissenbaum, H. (2010). *Privacy in context technology, policy and integrity of social life*. Stanford, CA: Stanford University Press.

Nosowitz, D. (2011, March 1). Everything you need to know about near field communication. *Popular Science Magazine*. Retrieved from Popular Science website: http://www.popsci.com/gadgets/article/2011-02/near-field-communication-helping-your-smartphone-replace-your-wallet-2010/

NYSDOT. (2007, July 10). *Announces travel time signs in Staten Island*. Retrieved from https://www.nysdot.gov/portal/page/portal/news/press-releases/2007/2007-07-10

Obeid, H. R., Zantout, R. N., & Sibai, F. N. (2007). *License plate localization in ALPR system*. Innovations in Information Technology, IIT '07. 4th International Conference on, 486–490.

Office of Community Oriented Policing Services. U.S. Department of Justice. (2011, October). *The impact of the economic downturn on American policing*. Retrieved from http://www.cops.usdoj.gov/files/RIC/Publications/e101113406_Economic%20Impact.pdf

Orwell, G. (1949). *Nineteen eighty-four (1984)*. New York, NY: Harcourt Brace Jovanovich, Incorporated.

Oyama, K. (2006). E-mail privacy after United States v. Councilman: Legislative options for amending ECPA. *Berkeley Technology Law Journal*, *21*, 499.

Ozer, N. A., & Schlosberg, M. (2007, August). *Under the watchful eye the proliferation of surveillance systems in California*. Retrieved from The California ACLU Affiliates website: www.aclung.org

Parfit, D. (1986). *Reasons and persons*. Oxford U.K.: Oxford University Press.

Patrick, R. (2012, January 24*). Effect of high court's GPS decision is uncertain in St. Louis case*. Retrieved from St. Louis Post-Dispatch website: http://www.stltoday.com/news/local/crime-and-courts/effect-of-high-court-s-gps-decision-is-uncertain-in/article_a7ced332-1229-5ff7-8669-0e75387f035b.html

Paul, I. (2011, June 9). *Facebook photo tagging: A privacy guide*. Retrieved from PC Word website: http://www.pcworld.com/article/229870 /facebook_photo_tagging_a_privacy_guide.html

Perin, M. (2011, April). Click, you're it. *Law Enforcement Technology*, *38*(4), 10–16. Retrieved from Law Enforcement Technology website: http://let.epubxpress.com/wps/portal/let/c1/04_SB8K8xLLM9MSSzPy8xBz9CP0os3iLkCAPEzcPIwMDFy9LA093F28jEwtHQ3cXM_2CbEdFABPvooM!/

Peters, T. A. (1999). *Computerized monitoring and online privacy*. New York, NY: McFarland & Company, Inc.

Pham, N. D. (2011, June). *The economic benefits of commercial GPS use in the U.S. and the costs of potential disruption*. Retrieved from the NDP Consulting website: http://www.saveourgps.org/pdf/GPS-Report-June-22-2011.pdf

Phillips, P. J., Scruggs, W. T., O'Toole, A. J., Flynn, P. J., Bowyer, K. W., Schott, C. L., & Sharpe. M. (2007, March 29). *FRVT 2006 and ICE large-scale result*. Retrieved from The Naval Postgraduate School Center for Homeland Defense and Security website: https://www.hsdl.org/?view&doc=75237&coll=limited

Planet Biometrics. (2013, January 17). *Invisible fingerprint recognition on smartphones*. Retrieved from http://www.planetbiometrics.com/article-details/i/1437/

Plourde-Cole, H. (2010, December). Note: Back to Katz: Reasonable expectation of privacy in the Facebook age. *Fordham Urban Law Journal*, *38*, 571–627.

Posen, D. E. (2005). The mosaic theory, national security, and the freedom of information act. *The Yale Law Journal*, *15*, 628–679. Retrieved from Yale Law Journal website: http://www.yalelawjournal.org/images/pdfs/358.pdf

Preston, J. (2011, January 14). *Homeland security cancels 'virtual fence' after $1 billion is spent*. Retrieved from The New York Times website: http://www.nytimes.com/2011/01/15/us/politics/15fence.html

The Privacy Act of 1974, as amended 5 U.S.C. § 552a.

Privacy and biometrics: Building a conceptual foundation. (2006, September 15). Retrieved from the Naval Postgraduate School Center for Homeland Defense and Security, Homeland Security Digital Library website: https://www.hsdl.org/?view&doc=85318&coll=documents

Privacy impact assessments. (2010, June). The Privacy Office Official Guidance. Department of Homeland Security.

Privacy International. (2007, December 28). *Leading surveillance societies in the EU and the world*. Retrieved from https://www.privacyinternational.org/article/leading-surveillance-societies-eu-and-world-2007

Privacy Rights Clearing House. (2013). *Fact sheet 8a: HIPAA basics: Medical privacy in an information age*. Retrieved from https://www.privacyrights.org/fs/fs8a-hipaa.htm

Prototype portable LPR system provides options. (2012, Fall). Retrieved from TechBeat website: https://www.justnet.org/pdf/Prototype-Portable-LPR-System-Provides-Options.pdf

Recent Cases. (2011a). D.C. circuit deems warrantless use of a GPS device an unreasonable search. *Harvard Law Review*, *124*(3), 827–834.

Recent Cases. (2011b). Third circuit allows government to acquire cell phone data without probable cause. —in re the application of the United States for an order directing a provider of electronic communication service to disclose records to the government, 620 F.3d 304 (3d Cir. 2010). *Harvard Law Review*, *123*(6), 1580–1587.

Ringland, K. (2009, Winter). The European Union's data retention directive and the United States's data preservation laws: Finding the better model. *Shidler Journal of Law, Commerce and Technology*, *5*.

Robison, W. J. (2010). Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act. *Georgetown Law Journal*, *98*, 1195.

Rosen, R. J. (2012, January 23). *Why the Jones Supreme Court ruling on GPS tracking is worse than it sounds*. Retrieved from the Atlantic website: http://www.theatlantic.com/technology/archive/2012/01/why-the-jones-supreme-court-ruling-on-gps-tracking-is-worse-than-it-sounds/251838/

Rubenfeld, J. (2008, January 1). *The end of privacy. Faculty scholarship series. Paper 1552*. Retrieved from Yale Law School, Lillian Goldman Law Library website: http://digitalcommons.law.yale.edu/fss_papers/1552

Rule, J. B. (2007). *Privacy in peril: how we are sacrificing a fundamental right in exchange for security and convenience*. New York, NY: Oxford University Press.

Salzmann, V. S. (2000, Winter). Are public records really public? The collision between the right to privacy and the disclosure of court records over the internet. *Baylor Law Review, 52,* 355–380.

Sanchez, J. (2010, August 11). GPS tracking and a 'mosaic theory' of government searches. [Web log post]. Retrieved from CATO Institute website: http://www.cato-at-liberty.org/gps-tracking-and-a-mosaic-theory-of-government-searches/

Savage, C. (2012, November 29). *Panel approves a bill to safeguard e-mail*. Retrieved from The New York Times website: http://www.nytimes.com/2012/11/30/technology/senate-committee-approves-stricter-privacy-for-e-mail.html?_r=0

Saylor, J. (2011, May). Computers as castles: Preventing the plain view doctrine from becoming a vehicle for overbroad digital searches. *Fordham University Law Review, 79*(6), 2809–2858. Retrieved from the Fordham University Law Review website: http://www.fordhamlawreview.org/articles/computers-as-castles-preventing-the-plain-view-doctrine-from-becoming-a-vehicle-for-overbroad-digital-searches

Schumacher, J. E., & Slobogin, C. (1993). Reasonable expectations of privacy and autonomy in fourth amendment cases: An empirical look at "understandings" recognized and permitted by society. *Duke Law Journal, 42*, 727–775. Retrieved from Duke Law Journal website: http://scholarship.law.duke.edu/dlj/vol42/iss4/1

Schwartz, J., (2001, September 5). As big PC brother watches, users encounter frustration, *New York Times,* C6.

Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *N.Y.U. L. Rev*., *86,* 1814, 1821.

Scott, C. (2012, May 14). *Facebook privacy head suggests company will serve ads on other sites*. Retrieved from PCWorld Business Center website: http://www.pcworld.com/businesscenter/article/255579/facebook_privacy_head_suggests_company_will_serve_ads_on_other_sites.html

Secure identification: The real ID act's minimum standards for driver's licenses and identification cards. Hearing before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, House of Representatives. 112th Cong., 2nd Sess. (2012). Retrieved from http://judiciary.house.gov/hearings/printers/112th/112-103_73416.PDF.

Seifert, D. (2011, July 14). *Police to use iPhones to identify perps*. Retrieved from Mobile Burn website: http://www.mobileburn.com/news.jsp?Id=15807

Serwin, A. B. (2009). Privacy 3.0-the principle of proportionality. *U. Mich. J. L. Reform*, *42*, 869.

Seuschek, H. (2010). *Applications for secure RFID in public safety*. Retrieved from European Commission Joint Research Center website: http://sta.jrc.ec.europa.eu/corsa/Workshop_for_Interoperable_communication/2010_06_29_Seuschek_Secure_RFID_Tracking_Technologies_b.pdf

Shaffer, G. (2000, Winter). Globalization and social protection: The impact of the EU and international rules in the ratcheting up of U.S. data privacy standards. *Yale Journal of International Law, 25.* Retrieved from Selected Works website: http://works.bepress.com/cgi/viewcontent.cgi?article=1002&context=gregory_shaffer&sei-redir=1&referer=http%3A%2F%2Fscholar.google.co.uk%2Fscholar%3Fq%3Dthe%2BData%2BProtection%2BAct%252C%2BData%2BProtection%2BAct%2B1998%2Bc.%2B29%252C%2B%26hl%3Den%26btnG%3DSearch%26as_sdt%3D1%252C14#search=%22Data%20Protection%20Act%2C%20Data%20Protection%20Act%201998%20c.%2029%2C%22

Shah, R. (2009, Spring). Recent development: From beepers to GPS: Can the fourth amendment keep up with electronic tracking technology. *University of Illinois Journal of Law, Technology & Policy,* 281–294.

Sheridan, T. I. III. (1975). Electronic Intelligence Gathering and the Omnibus Crime Control and Safe Streets Act of 1968. *Fordham Law Review*, *44*(2), 331. Retrieved from Fordham Law Review website: http://ir.lawnet.fordham.edu/flr/vol44/iss2/5

Shih, G. (2012, February 10). *Path's fumble highlights internet privacy concerns*. Retrieved from Reuters website: http://www.reuters.com/article/2012/02/10/us-socialmedia-privacy-path-idUSTRE81826X20120210

Sledge, M. (2012, November 29). *ECPA amendment passes, as senate judiciary votes to require warrant for email snooping*. Retrieved from Huffington Post website: http://www.huffingtonpost.com/2012/11/29/ecpa-electronic-communications-privacy-act_n_2211889.html

Slobogin, C. (2007). *Privacy at risk: The new government surveillance and the fourth amendment*. Chicago, IL: University of Chicago Press.

Smith, A. (2011, February 28). *Law enforcement use of global positioning (GPS) devices to monitor motor vehicles: Fourth amendment considerations*. (Congressional Report No. R41663). Washington DC: Library of Congress Congressional Research Service. Retrieved from Open CRS website: http://www.fas.org/sgp/crs/misc/R41663.pdf

Solove, D. J. (2002). Access and aggregation: Privacy, public records and the constitution. *Minnesota Law Review*, *86*(6). Retrieved from Social Science Research Network website: http://ssrn.com/abstract=283924/ or doi:10.2139/ssrn.283924

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age.* New York, NY: New York University Press.

Solove, D. J. (2006a). *A brief history of information law privacy law*. Retrieved from Social Science Research Network website: http://ssrn.com/abstract=914271

Solove, D. J. (2006b). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564.

Solove, D. J. (2010). Fourth amendment pragmatism. *Boston College Law Review*, *51*, 1511–1538.

Spy files. (n.d.). Retrieved from The American Civil Liberties Union website: http://www.aclu.org/spy-files

Stanley, J., & Steinhardt, B. (2003, January). *Bigger monster, weaker chains: The growth of an American surveillance society*. ACLU Technology and Liberty Program.

StarChase covert tracking system. (n.d.). Retrieved from http://www.starchase.com/SC-Covert-User-Directions-Spec-Sheet.pdf

State of Illinois, Roads and Bridges, (605 ILCS 10/) Toll Highway Act.

Steele, E. (2011, July 13). *How a new police tool for face recognition works*. Retrieved from The Wall Street Journal website: http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works/

Stevens, G. M. (2003, March 21). *Privacy: Total information awareness programs and related information access, collection, and protection laws* (Congressional Report No. RL31730). Washington DC: Library of Congress Congressional Research Service.

Stored Communications Act (18 U.S.C. §§ 2701–2712).

Strandburg, K. (2011). Home, home on the web and other fourth amendment implications of technosocial change. *Maryland Law Review*, *70*, 614.

Strandburg, K. J. (2008). Freedom of association in a networked world: First Amendment regulation of relational surveillance. *British Columbia Law Review, 49,* 741. Retrieved from Digital Commons@Boston College Law School website: http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=2389&context=bclr&sei-redir=1#search=%22Katherine%20J.%20Strandburg%2C%20Freedom%20Association%20Networked%20World%3A%20First%20Amendment%20Regulation%20Relational%20Surveillance%2C%2049%20B.C.%20L.%20Rev.%20741%2C%20769%E2%80%9377%20%282008%29%20%28arguing%20Fourth%20Amendment%20provides%20insufficient%20protection%20against%20government%20%E2%80%9Crelational%20surveillance%E2%80%9D%20using%20traffic%20data%29.%22

Stratford, J. S., & Stratford, J. (1998, Fall). Data protection and privacy in the United States and Europe. *IASSIST Quarterly*, 17–20. Retrieved from International Association for Social Science Information Services & Technology website: http://www.iassistdata.org/downloads/iqvol223stratford.pdf

Taylor, N. (2002). State surveillance and the right to privacy. *Surveillance & Society, 1*(1), 66–85. Retrieved Surveillance & Society website: http://www.surveillance-and-society.org/articles1/statesurv.pdf

Taylor, N. (2011, September 5). A conceptual legal framework for privacy, accountability and transparency in visual surveillance systems. *Surveillance & Society, 8*(4). Retrieved from Surveillance & Society website: http://www.surveillance-and-society.org/ojs/index.php/journal/article/view/conceptual

Thangavelu, A. (2007, February 22–24). *Location identification and vehicle tracking using VANET (VETRAC),* 112–116. Retrieved from Academia.edu website: http://vit.academia.edu/ArunkumarThangavelu/Papers/112889/Location_Identification_and_Vehicle_Tracking_using_VANET_VETRAC_

Thomas, C. (2007, January). *Connecting the dots*. Retrieved from Public Works Magazine website: http://www.pwmag.com/bim/connecting-the-dots.aspx

Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Pub. L. No 90-351, § 802, 82 Stat. 212. 18 U.S.C. §§ 2510, et al. (1968, 2010).

Transportation Security Administration. (n.d). *Innovation and technology. About TSA.* Retrieved from http://www.tsa.gov/about-tsa/innovation-and-technology

Transportation Security Administration. (2008, February). *Strategic solutions*. Retrieved from www.tsa.gov/approach/tech/

TxTag. (n.d.). Retrieved from Texas Tollway Authority website: http://www.txtag.org/register.php

U.S. Customs and Border Patrol. (2009, December). *SBInet block 1*. Retrieved from http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/border/secure_border/

U.S. Department of Health and Human Services. (n.d). *Health information privacy. Summary of the HIPPA privacy rule.* Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

United States attorneys manual (USAM). (1997). Retrieved from The United States Department of Justice website; http://www.justice.gov/usao/eousa /foia_reading_room/usam/index.html

United States Court. (n.d.). *Courts of appeals.* Retrieved from http://www.uscourts.gov/FederalCourts/UnderstandingtheFederalCourts/CourtofAppeals.aspx

Vieth, P. J. (2011, June 22). Bill: Warrant would be needed for GPS tracking. *Virginia Lawyers Weekly.*

Wafa, T. (2010, Summer). How the Lack of Prescriptive Technical Granularity in HIPAA Has Compromised Patient Privacy. *Northern Illinois University Law Review, 30*(3). Retrieved from Northern Illinois University Law Review website: http://www.niu.edu/law/organizations/law_review/pdfs/full_issues/30_3/Wafa.pdf

Walton, Z. (2012, August 2). *Cybersecurity Act of 2012 killed in the Senate*. Retrieved from WebPro News website: http://www.webpronews.com/cybersecurity-act-of-2012-killed-by-the-senate-2012-08

Webb, J. P. (2011–2012, Winter). Car-ving out notions of privacy: The impact of GPS tracking and why Maynard is a move in the right direction. *Marquette Law Review, 95*, 751.

Webster, W. R. (2004). The diffusion, regulation and governance of closed-circuit television in the UK. *Surveillance & Society, 2*(2/3). Retrieved from Surveillance & Society website: http://www.surveillance-and-society.org/articles2(2)/diffusion.pdf

Welcome. (n.d.). Retrieved from Techlawjournal website: http://www.techlawjournal.com/welcome.htm

Wells, R. B. (2009, October). Comment: The fog of cloud computing: Fourth amendment issues raised by the blurring of online and offline content. *University of Pennsylvania Journal of Constitutional Law, 12*, 223–240.

Wichmann III, C. J. (1998). Ridding FOIA of those "unanticipated consequences": Repaving a necessary road to freedom. *Duke Law Journal, 47,* 1213.

Wilson, T. J., & Woodard, P. F. (1987, April). *Automated fingerprint identification systems: Technology and policy issues*. Retrieved from Simson Garfinkel's website: http://simson.net/ref/1987/NCJ-104342_AFIS.pdf

Woodard, J. D. (1998). *Biometrics: Identifying law & policy concerns. Chapter 19.* Retrieved from Michigan State University, Department of Computer Science and Engineering website: http://www.cse.msu.edu/~cse891/Sect601/textbook/19.pdf

Yinger, C. H. (2002, Summer). Operation and application of the global positioning system. *Satellite Navigation, 3*(2). Retrieved from Aerospace website: http://www.aero.org/publications/crosslink/summer2002/02.html

Zoufal, D. R. (2008). *Someone to watch over me* (master's thesis). Naval Postgraduate School, Monterey, CA.

Cases Cited

Alexander v. F.B.I. 971 F. Supp. 603 (D.D.C. 1997)

Bechhoefer v. U.S. Dept. of Justice D.E.A. 209 F.3d 57 (2d Cir. 2000)

Berger v. New York 388 U.S. 41 (1967)

Board of Public Instruction of Broward County v. Doran 224 So. 2d 693 (Fla. 1969)

Bond v. United States 529 U.S. 334, 120 S. Ct. 1462 (2000)

Case of Peck v. United Kingdom. Application no. 44647/98. pp. 10–15. Strasbourg (January 28, 2003)

City of Ontario v. Quon 130 S. Ct. 2619 (2010)

Commonwealth v. Connolly 913 N.E.2d 356 (Mass. 2009)

County of Santa Clara v. Superior Court 170 Cal. App. 4th 1301 (2009)

Davis v. Mississippi 394 U.S. 721 (1969)

Florida v. Riley 488 U.S. 445 (1989)

Goodman v. Liebovitz 410 N.Y.S.2d 502 (1978) aff'd, 423 N.Y.S.2d 488 (1980)

Griswold v. Connecticut 381 U.S. 479 (1965)

Guest v. Leis 255 F.3d 325 (6th Cir. 2001)

Illinois v. Caballes 543 U.S. 405 (2005)

In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to Government 620 F.3d 304 (3d Cir. 2010)

In re Grand Jury Proceedings 827 F.2d 301 (8th Cir. 1987)

Katz v. United States 389 U.S. 347 (1967)

King v. United States 55 F.3rd 1193 (6th Cir. 1995)

Kyllo v. United States 533 U.S. 27 (2001)

Lawrence Et al v. Texas 539 U.S. 558 (2003)

Lewis v. United States 385 U.S. 206 (1966)

Oliver v. United States 466 U.S. 170 (1984)

Olmstead v. United States 277 U. S. 438 (1928)

People v. Weaver 909 N.E.2d 1195 (N.Y. 2009)

Pineda-Moreno v. United States 132 S. Ct. 1533 (2012)

Planned Parenthood of Se. Pennsylvania v. Casey 505 U.S. 833 (1992)

Rios v. United States 364 U. S. 253 (1960)

Roe v. Wade 410 U.S. 113 (1973)

Schmitt v. City of Detroit 395 F.3d 327 (6th Cir. 2005).

Skinner v. Railway Labor Executives' Association 489 U.S. 602 (1989)

Smith v. Maryland 442 U.S. 735 (1979)

State v. Young 867 P.2d 593 (1994)

United States Department of Justice v. Reporters Committee for Freedom of Press 489 U.S. 749 (1989)

United States v. Amaral-Estrada 509 F.3d 820 (7th Cir. 2007)

United States v. Amaya CR 11-4065-MWB, 2012 WL 1188456 (N.D. Iowa Apr. 10, 2012) opinion withdrawn in part on reconsideration, CR 11-4065-MWB, 2012 WL 1523045 (N.D. Iowa May 1, 2012)

United States v. Bermudez 2006 WL 3197181 (S.D. Ind. June 30, 2006), aff'd 509 F.3d 820 (7th Cir. 2007)

United States v. Castillo-Garcia 117 F.3d 1179 (10th Cir. 1997)

United States v. Cuervas-Perez 640 F.3d 272 (2011)

United States v. Flores-Lopez 670 F.3d 803 (7th Cir. 2012)

United States v. Forrester 512 F.3d 500, 510 (9th Cir. 2007)

United States v. Fregoso 60 F.3d 1314 (8th Cir. 1995)

United States v. Garcia 474 F.3d 994 (7th Cir. 2007)

United States v. Giordano 416 U.S. 505, 528 (1974)

United States v. Hambrick 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) aff'd, 225 F.3d 656 (4th Cir. 2000)

United States v. Hernandez, ___ F.3d ___, 2011 U.S. LEXIS 14659 (2011)

United States v. Horowitz 806 F.2d 1222 (4th Cir. 1986)

United States v. Jones 132 S. Ct. 945 (2012)

United States v. Karo 468 U.S. 705 (1984)

United States v. Knotts 460 U.S. 276 (1983)

United States v. Marquez 605 F.3d 604 (8th Cir. 2010)

United States v. Maynard 615 F.3d 544 (D.C. Cir. 2010)

United States v. McIver 186 F.3d 1119 (9th Cir. 1999)

United States v. Miller 425 U.S. 435 (1976)

United States v. Moran 349 F. Supp.2d 425 (N.D.N.Y. 2005)

United States v. New York Telephone Company 434 U.S. 159 (1977)

United States v. Nowka 5:11-CR-00474-VEH, 2012 WL 2862139 (N.D. Ala. May 14, 2012)

United States v. Perrine 518 F.3d 1196 (10th Cir. 2008)

United States v. Pineda-Moreno 591 F.3d 1212 (9th Cir. 2010) cert. granted, judgment vacated, 132 S. Ct. 1533, 182 L. Ed. 2d 151 (U.S. 2012)

United States v. Pineda-Moreno 688 F.3d 1087 (9th Cir. 2012) cert. denied, 12-7799, 2013 WL 215669 (U.S. Jan. 22, 2013)

United States v. Skinner 690 F.3d 772 (6th Cir. 2012)

United States v. Torres 751 F.2d 875 (7th Cir. 1984)

Whalen v. Roe 429 U.S. 589 (1977)

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California