PRIVACY-INVADING TECHNOLOGIES AND RECOMMENDATIONS FOR DESIGNING A BETTER FUTURE FOR PRIVACY RIGHTS

ALEXANDRA RENGEL*

Introduction

The concept of privacy has been discussed for centuries by philosophers, anthropologists, sociologists, and legal scholars.[1] The importance that individuals place on privacy is beyond question and transcends geographical, cultural and racial boundaries. Individuals' need for secrecy and private space is so fundamental to forging relationships with others, and to preserving our sense of self, that a society with a complete lack of individual privacy would be

* Alexandra I. Rengel is the author of PRIVACY IN THE 21ST CENTURY (Martinus Nijhoff Publishers 2013). She is an attorney in private practice in the law firm of Mercado & Rengel. Ms. Rengel received her B.A. from Mount Holyoke College and earned her J.D. from Boston University School of Law. Ms. Rengel is a *summa cum laude* graduate and valedictorian of the St. Thomas University School of Law LL.M. Program in Intercultural Human Rights. She also obtained her J.S.D. at St. Thomas University School of Law, writing her dissertation on the right to privacy in the international context, for which she earned the grade of *summa cum laude*. In this article, the author draws freely on sections of this book. Ms. Rengel teaches at Schiller International University in Madrid and at Comillas Pontifical University in Madrid. She is also a frequent lecturer on human rights, international business law and arbitration. Ms. Rengel writes this article with special thanks to her husband Ivan Mercado.

[1] *See* Cao Jingchun, *Protecting the Right to Privacy in China*, 36 VICT. U. WELLINGTON L. REV. 645, 646-47 (Oct. 2005) (stating that privacy was protected, to some extent, in ancient China and an awareness of privacy may be found in the Warring States Period, referring to the era of about 475 BC to 221 BC); JUDITH A. SWANSON, THE PUBLIC AND PRIVATE IN ARISTOTLE'S POLITICAL PHILOSOPHY 207 (1992); BARRINGTON MOORE, PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY (1984); MARGARET MEAD, COMING OF AGE IN SAMOA: A PSYCHOLOGICAL STUDY OF PRIMITIVE YOUTH FOR WESTERN CIVILIZATION 219 (1973) (explaining that Margaret Mead's studies of Samoan culture revealed that even though children were raised by village members and exposed to all aspects of life in the public arena, their first act of sexual intercourse took place in privacy).

unimaginable.[2] A right to privacy protects individuals from having the contents of certain private information made public and regulates the means and manner by which that information is obtained.[3] However, new technologies often make us wonder what level of protection for our right to privacy is possible in our world where personal information about us can easily be accessed without the need to infringe into our physical space, but by invisible hands that can get to know our most private secrets with a keystroke and looking at a screen. As technology becomes increasingly able to facilitate breaches in our privacy, it becomes most important to establish protections.

In the last thirty years, extraordinary events[4] have made us reconsider the concept of privacy. Globalization and the digital age[5] have affected humanity and continue to advance at such a rapid rate that what the future will bring is difficult to imagine. Today, fast-paced innovation and perpetual change is the only constant, and it can be said that the digital age with all of its technological developments has changed the world. The Internet, social networks, large storing systems, as well as sophisticated electronic sharing and communication devices, allow for the fast transfer of information and smooth the progress of communication between people around the

---

[2] Charles Fried, *Privacy*, 77 YALE L.J. 475 (1968) (arguing that in developed social contexts love, friendship, and trust are only possible if persons enjoy and accord to each other a certain measure of privacy).

[3] In a comprehensive review of literature published in 1995, psychologist Patricia Brierley Newell identified at least seventeen discrete concepts of privacy. These included describing privacy as a phenomenal state or condition of the person, a quality of place, a space of refuge, a goal, a descriptor of personal space or territoriality, a level of close personal intimacy, a behavior, a process, a legal right, a descriptor of an interactive condition (such as an attitude, solitude, anonymity, and secrecy), and the ability to control information, among others. *See* Patricia Brierley Newell, *Perspectives on Privacy*, 15 J. ENVTL. PSYCHOL. 87 (1995).

[4] These include the advent of the Internet, the growth of social media, threats from terrorism, and new technologies that allow for data mining and collection.

[5] *Digital Age Definition*, CAMBRIDGE BUSINESS ENGLISH DICTIONARY http://dictionary.cambridge.org/dictionary/business-english/digital-age (last visited June 12, 2013) ("The present time, when most information is in a digital form, especially when compared to the time when computers were not used.").

world. In addition to the advancements in the communication field, surveillance technologies have also become highly developed, are now less expensive, easier to obtain and less noticeable.[6] Today, not only governments, but also private individuals have access to surveillance systems that were previously reserved to books of science fiction.[7] Concern for privacy has become an issue in the most innocuous of transactions, such as standing in a public place where Closed Circuit Television (CCTV) cameras might be installed, doing a search on Google, making travel reservations, paying bills through online banking, or even checking out a library book.[8] Technology has removed all geographical restrictions for these once private acts, which are now accessible by private parties, the public and the government - all from the most remote of locations.[9] At this time, it is essential to consider the effect of these new technologies on privacy and to deem it vital that legislators, politicians, designers and manufacturers take an active role in protecting privacy rights.

There are initiatives that can be undertaken to design a future digital landscape for the world that makes the most of the positive

---

[6] Today, things such as GPS, geolocation, CCTV and mass storage allow for cheap and effective collection and retention of data and other information. *See* TOBY MENDEL ET. AL., GLOBAL SURVEY ON INTERNET PRIVACY AND FREEDOM OF EXPRESSION 14-17 (2012), *available at* http://unesdoc.unesco.org/images/0021/002182/218273e.pdf.

[7] Ever more sophisticated and cheaper CCTV cameras are being used by private citizens and companies. *See* Robert Marchant, *Surveillance society puts cameras in more locations*, USA TODAY ONLINE (June 10, 2013), http://www.usatoday.com/story/news/nation/2013/06/10/surveillance-society-cameras-public-locations/2409893/. There are also wearable devices that could severely infringe on privacy. *See* Claire Cain Miller, *Lawmakers Show Concerns About Google's New Glasses*, N.Y. TIMES (May 17, 2003), http://www.nytimes.com/2013/05/17/technology/lawmakers-pose-questions-on-google-glass.html?_r=0.

[8] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1394 (2001) [hereinafter Solove, *Privacy and Power*].

[9] *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1468-1501 (2000); Will Thomas DeVries, *Note, Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 291 (2003); Jerry Berman & Deirdre Mulligan, *The Internet and the Law: Privacy in the Digital Age: A Work in Progress*, 23 NOVA L. REV. 549, 555 (1999).

effects of technology while taking into account privacy concerns. A good starting point is to appreciate that the laws need to catch up with the technology in order to adequately protect individuals' privacy. Legislators need to be advised by experts knowledgeable about the technology they are attempting to legislate in order for the laws to be effective. We can also rely on the designers and manufacturers of technology to consider the ethical implications of the technology they create. The technology and the ease of communications in today's world have helped individuals recognize that the concept of privacy is more than an abstract notion, and that we must actively seek its protection in order to enjoy the type of freedom that society strives to reach. Value Sensitive Design,[10] Privacy by Design,[11] and Privacy-Enhancing Technologies,[12] are all

[10] Value Sensitive Design (VSD) is a theoretically grounded approach based on aiming to control or regulate the intrusive capabilities of the technologies concerned and embedding ethics and human values in a principled and comprehensive manner in the design and manufacture of technology law alone. *See* Alan Sorning, Satya Friedman & Peter H. Kahn, Jr., *Designing for Human Values in an Urban Simulation System: Value Sensitive Design and Participatory Design*, *in* SHORT PAPERS, EIGHTH BIENNIAL PARTICIPATORY DESIGN CONFERENCE 68-69 (2004), *available at* https://ojs.ruc.dk/index.php/pdc/article/download/317/309 (discussing development of value added design and its applicability to respecting human values).

[11] As to privacy-invading technologies, "privacy by design" promotes designing information and communications technologies (ICT) and building privacy into the product or technology from the outset. *See* Ann Cavoukian, *Privacy by Design*, INFO. & PRIVACY COMM'R 1 (2009), http://www.ipc.on.ca/images/Resources/privacybydesign.pdf (stating that she "first developed the term 'Privacy by Design' back in the '90s" and that "'Build in privacy from the outset' has been [her] longstanding mantra, to 'avoid making costly mistakes later on, requiring expensive retrofits").

[12] Privacy-Enhancing Technologies (PETs) are applications or tools with discrete goals that address a single dimension of privacy, such as anonymity, confidentiality, or control over personal information. Frequently, PETs are added onto existing systems, sometimes as an afterthought by designers and sometimes by privacy-sensitive end-users. *See* Jim Brock, *Are Privacy Add-Ons Effective? Surprising Results from Our Testing*, PRIVACYCHOICE (Nov. 17, 2010), http://blog.privacychoice.org/2010/11/17/are-privacy-add-ons-effectivesurprising-results-from-our-testing/ (comparing the effectiveness of a single type of privacy add-on that blocks efforts by data and marketing companies to track online activity).

the result of concern about the effect of new technologies on privacy, and are all positive signs that reflect on humans' value of privacy and other fundamental rights.

I. Privacy in the Digital World

The realization about the lack of privacy in today's world can happen as easily as when a party host realizes people, who had not been invited to a party, have found out about the event from invitees posting pictures on Facebook or Twitter. Something about such an occurrence, as it relates to privacy, feels intuitively wrong, perhaps because a human's need for individual privacy can be described as being innate.[13] People have a sense that there are aspects of life and themselves that they have a right to keep private.[14] Privacy is a

[13] It is understood, however, that although intuitively everyone needs some degree of privacy, our intuitions vary, and the areas of privacy that we value might differ depending on our cultural values. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1160 (2004). As James Whitman points out, "[w]e have intuitions that are shaped by the prevailing legal and social values of the societies in which we live. In particular, we have, if I may use a clumsy phrase, *juridified* intuitions − intuitions that reflect our knowledge of, and commitment to, the basic legal values of our culture." *Id.* In his well-reasoned article, Whitman examines the differences in the understanding of the concept of privacy in the United States and Europe and observes that while American privacy law protects individual liberty against the State, European privacy law promotes dignity in interpersonal relations. *Id.* at 1160-62. What is most relevant, however, is that while our definition of privacy may vary, it is undeniable that the need for some degree of individual privacy is present in our consciousness from the time we are able to think. *Id.* at 1160-63.

[14] Clearly, cultural norms will influence a society's privacy customs, and in some primitive societies, where group survival is more important than individual privacy, there is less emphasis on an individual's space. However, anthropological studies have shown that even in some societies where privacy was not a recognized value, there were instances where members required privacy from the others, such as when engaged in their first act of sexual intercourse. MEAD, *supra* note 1, at 219-20 (revealing that children were raised by village members and exposed to all aspects of life in the public arena with the exception of when they engaged in their first act of sexual intercourse). *See also,* Susan P. Stuart, *Fun with Dick and Jane and Lawrence: A Primer on Education Privacy as Constitutional Liberty*, 88 MARQ. L. REV. 563 (2004) (discussing the findings of Margaret Mead and

prerequisite for humans' most basic interactions with each other, and most societies regard some areas of human activity as being not suitable for general observation and knowledge.[15] Nevertheless, today's technology makes it very difficult to keep certain things private and allows accessibility to private information much easier than ever before. It seems as if technology is taking away humans' ability to protect their privacy.

The acknowledgement that humans have the need to protect their privacy began early in our legal history; legal protections for the right to privacy have evolved depending on the specific needs of the time and the legal traditions of the various geographical areas where the law has developed. Whether as a response to having an image published, or to having personal financial information compromised, the law has responded by offering protection to individuals.[16] Interestingly, privacy protections have appeared since Antiquity in the majority of legal systems of the world, regardless of their diverse legal traditions. Unfortunately, as the means and methods used to encroach upon privacy have evolved and continue to become ever more sophisticated, the law has often had to play catch-up to the ever-evolving invasions of individuals' privacy. The wide-ranging scenarios in which privacy concerns are implicated have also added to the difficulty inherent in protecting and respecting privacy. Today, privacy continues to be a fertile ground for legal development.

The need for the specific legal protection of the right to privacy has been exacerbated by the development of new communication and information technologies that facilitate the invasion and interference with an individual's privacy. One of the

---

proposes that the more primitive the society, the less emphasis there is on privacy).

[15] MEAD, *supra* note 1, at 124-25, 219, 290.

[16] The European Union's Data Privacy Directive (EU Data Protection Directive (95/46/EC)), provides a broad scheme intended to provide protection to private citizens and their personal information. Various Latin American countries have implemented a concept known as *habeas data* to grant remedies for data protection violations; these countries include Brazil, Argentina, Paraguay, Peru and Mexico. *See* Andres Guadamuz, *Habeas Data: The Latin-American Response to Data Protection*, 2000 (2) J. INFORMATION, LAW AND TECHNOLOGY (JILT), *available at* http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html.

most important "effects of global industrialization has been the transformation of technologies of communication."[17] The amount of personal information that could be collected in the pre-computer era was determined by practical considerations, such as the difficulty involved in collecting the data and the physical space required for storing it. Today, however, digitized information is stored electronically in computer databases, take up relatively little physical storage space, and can be collected with relative ease on a massive scale from remote locations.[18] The speed at which information can be exchanged between databases has also changed dramatically. In the pre-computer era, records had to be physically transported between filing destinations. The time it took to move the information depended upon the transportation systems that carried the physical records. Now records can be transferred between electronic databases in milliseconds through high-speed cable or even fiber optic lines.[19] As to the length of time information could be stored: before the information era, data was manually recorded and stored in file cabinets, shelves, or other storage locations and then placed in larger physical repositories. For practical reasons, that information could only be retained for a limited amount of time, and could not be preserved indefinitely without great expense and effort.[20] In the last few years, databases of personal information have grown exponentially in number and in variety.[21] The capability of storage of these new digital data depositories is massive, there is virtually no limit on how much information can be stored or on how long it can be retained.[22] Many of the technologies used for storage and data collection are based on digital wireless communications, and personal information routinely flows across jurisdictional boundaries. Geography, therefore, is no longer an obstacle in

---

[17] ANTHONY GIDDENS, THE CONSEQUENCES OF MODERNITY 70 (1991).

[18] *See* Ethan Katsh, *Law in a Digital World: Computer Networks and Cyberspace*, 38 VILL. L. REV. 403, 423-24 (1993).

[19] *Id.* at 416.

[20] In this regard we should consider institutions such as libraries or archives where millions of documents had to be stored and preserved using both physical space and other resources.

[21] *See* Solove, *Privacy and Power*, *supra* note 8, at 1401-06.

[22] *See Id.*

obtaining and storing data. New technologies have simply changed the way communication and information transfer take place. The people's concept of privacy and how to protect it has also changed.[23]

Within the context of the development of faster and more efficient communication and information transfers, the impact of new digital technologies on our everyday activities is unprecedented.[24] The last generation has seen technological change on a scale matching or exceeding that of the industrial revolution.[25] Three relatively recent major digital developments have affected our concept of privacy greatly: (1) the increase in data creation and the resulting collection of vast amounts of personal data—caused by the electronic recording of almost every transaction; (2) the globalization of the data market and the ability of anyone to collate and examine this data; and (3) the lack of the types of control mechanisms for digital data that existed to protect analog data.[26] These three developments all concern the changes wrought by digital technology on the ability to manipulate, store and disseminate information.

The amount of digital information the modern age has generated is extraordinary.[27] Every interaction with the Internet and with social networks, every credit card transaction, every bank withdrawal, and every magazine subscription is recorded digitally and linked to specific users. In the analog world, these transactions were either not recorded at all or recorded on paper in a single location; therefore, the information was not as easily accessible as it is today.[28] All of this information, once it is collected in networked

---

[23] Solove, *Privacy and Power*, *supra* note 8, at 1401-06.

[24] *See id.* at 1394 (describing the impact of digital technology on our day to day life such as how we bank, shop, and participate in other innocuous daily activities).

[25] *See* Eugene R. Quinn, Jr., *Tax Implications for Electronic Commerce over the Internet*, 43 J. TECH. L. & POL'Y 1, 50 (1999) (comparing the Industrial Revolution with the "digital revolution" and claims that the "digital revolution has the potential to cause societal change on a magnitude that is even greater than that caused by the Industrial Revolution").

[26] *See* Berman & Mulligan, *supra* note 9, at 553-54.

[27] Froomkin, *supra* note 9, at 1462.

[28] As compared to old-fashioned cash commerce, today's "e-commerce" allows merchants to track your "clickstream" through the use of "cookies," and

databases, can be sent instantly and inexpensively around the globe.[29] In this newly commoditized information market, buyers everywhere can collate and manipulate the data for marketing, profiling, and, in some instances, for nefarious purposes.[30] Individuals have little ability to control this collection or manipulation of their data. Not only does much of this happen far from the reach of regulators, but most people are not even aware of what information has been collected about them or for what purpose it is being used.[31]

While all of these changes affect the transfer of communication and information, not only informational privacy has been affected, autonomy is also imperiled from the interference with one's daily life by digital technology.[32] When almost every activity leaves a digital trail, government and private monitoring becomes less about analog surveillance or human intelligence gathering and more a matter of "data mining."[33] With these technological advancements there is also a corresponding increase in the risks to privacy.[34] The competing interests at play are the demands of a

---

they are able to track your interests based on what you view as well as what you purchase, while credit companies are able to record your purchase. *See* In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 501-05 (S.D.N.Y. 2001).

[29] *See* Berman & Mulligan, *supra* note 9, at 554.

[30] *See, e.g.* Perlroth Nicole, *Malware That Drains Your Bank Account Thriving on Facebook*, N.Y. TIMES, June 3, 2013, *available at* http://bits.blogs.nytimes.com/2013/06/03/malware-that-drains-your-bank-account-thriving-on-facebook/ (detailing data mining on popular social media site for personal information).

[31] *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1095 (July, 2002).

[32] As do other areas of privacy, *see generally* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996) (explaining how, for example, digital technology threatens the ability to participate anonymously in digital society because every digital interaction leaves personally identifiable fingerprints).

[33] *See generally* Joseph S. Fulda, *Data Mining and Privacy*, 11 ALB. L.J. SCI. & TECH. 105 (2000) (defining data mining as: "the intelligent search for new knowledge in existing masses of data"). Data mining shows how difficult it is to fully determine the various breaches of privacy because the technology allows the collection and potential for misuse of such vast amounts of data.

[34] *See* Solove, *supra* note 8, at 1393-94 (2001) (describing the impact of

democratic society and the need and appetite for electronic commerce and information technology, balanced against the reality that technologies that might be invasive of privacy also have the potential for unprecedented opportunities for enlightenment, prosperity and security. Traditionally, privacy law has developed in tandem with technology and has constantly reshaped itself to meet the privacy threats embodied in new technologies.[35] The information revolution, however, has been taking place at such a rapid speed, and affecting so many areas of privacy law, that the orthodox, adaptive legislative and judicial process has failed to address digital privacy problems adequately.[36] Specific examples of technology affecting individual privacy that have developed in recent years or have become more sophisticated are countless. A few examples follow.

II. Privacy-Invading Technologies

A. Biometrics

What is commonly referred to as biometrics is actually the operation of collecting, synthesizing and subsequently storing data relating to a particular individual's characteristics— physical, genetic or otherwise—for identification purposes.[37] The most commonly used types of biometric identifiers are generated from fingerprints, retina scanning, hand and palm geometrics, voice recognition, and digitized imagery.[38] Various forms of biometric technology are being used worldwide in such places as government agencies, education

---

digital technology on our day to day life such as how we bank, shop, and participate in other innocuous daily activities).

[35] *See* Dennis F. Hernandez, *Litigating the Right to Privacy: A Survey of Current Issues*, 446 PLI/PAT 425, 429 (1996).

[36] *See* Berman & Mulligan, *supra* note 9, at 554.

[37] *See* Rudy Ng, *Catching up to our Biometric Future: Fourth Amendment Privacy Rights and Biometric Identification Technology*, 28 HASTINGS COMM. & ENT. L.J. 425 (2006).

[38] Bridget Mallon, *"Every Breath You Take, Every Move You Make, I'll Be Watching You": The Use of Face Recognition Technology*, 48 VILL. L. REV. 955, 972 (2003).

centers, police departments, automated bank devices, and retail establishments.[39] The Russian government has announced its intention to implement an electronic system based on fingerprints for use in its banking system.[40] Individuals in Jamaica use thumb scan technology in polling stations during elections.[41] Other countries are seeking to implement biometric identifiers for non-governmental uses such as credit cards, as is the case of France and Germany, where such ideas have been discussed and tests are under way for using these new technologies.[42] In the United States (U.S.), the San Francisco International Airport has installed hand geometry identification stations for employees in some secure areas.[43] Before being allowed to proceed into restricted areas, employees must place their hand on a biometric reader, which scans their hand and compares it to images stored in a database.[44] In 2006, the public school system in Freehold, New Jersey, installed an iris scanning system in an effort to have better control of the school visitors who had access to school buildings.[45] Thirty-seven states use facial recognition systems designed to thwart identity theft by preventing fraudulent drivers' licenses.[46] Walt Disney World Corporation has been using biometrics to track ticket holders for years at their theme

---

[39] Mark G. Milone, *Biometric Surveillance: searching for Identity*, 57 BUS. LAW 497, 498-99 (November 2001).

[40] Privacy and Human Rights, *An International Survey of Privacy Laws and Practice*, GLOBAL INTERNET LIBERTY CAMPAIGN, *available at* www.gilc.org/privacy/survey/intro.html (last viewed Oct. 17, 2012).

[41] *Id.*

[42] *Id.*

[43] *See* Patricia Barnes, *Keeping Security Risks at Bay at San Francisco International Airport*, ACCESS CONTROL & SECURITY SYSTEMS (Aug. 1, 1997), *available at* http://securitysolutions.com/mag/security_keeping_security_risks/.

[44] *See id.*

[45] Laurie Sullivan, *Iris Scanning For New Jersey Grade School*, INFORMATION WEEK (Jan. 23, 2006), *available at* http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=177103030.

[46] *See* Craig Timberg, *State Photo-ID Databases Become Troves for Police*, WASH. POST (June 17, 2013), *available at* http://www.washingtonpost.com/business/technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497_story.htm.

parks worldwide.[47]

Vein pattern recognition (VPR) systems are amongst the fastest growing biometric technologies to have emerged in the recent past, and are being put to public, commercial and military use throughout the world.[48] It has been used extensively by financial institutions, and can now be found on PC's as a login device, as well as within hospitals and military facilities, as well as a tool in law enforcement.[49] Vein authentication uses the vascular patterns of an individual's palm/finger/back of the hand as personal identification data.[50] Veins and other subcutaneous features in the human hand present large, robust, stable and largely hidden patterns.[51] The deoxidized hemoglobin, located in the vein vessels, absorbs light having a wavelength in the near-infrared area.[52] When an infrared ray image is captured, only the blood vessel patterns containing the deoxidized hemoglobin are visible as a series of dark lines.[53] The vein authentication device translates the black lines of the infrared ray image, and then matches them with the previously registered pattern of the individual.[54] VPR technology consists of a small vein scanner—the users simply need to hold the palm/finger/back of hand a few centimeters over the scanner and the scanner reads the unique vein pattern.[55] Vein recognition works on the fact that everyone has distinct vein patterns. The technology functions by utilizing a kind of

---

[47] *See* Anil K. Jain, et al., *Fingerprint Matching*, IEEE COMPUTER SOCIETY, 41 (February 2010), *available at* http://biometrics.cse.msu.edu/Publications/Fingerprint/JainFpMatching_IEEEComp10.pdf.

[48] *See* Harvey McEwan, *Finger Vein Recognition*, EZINE ARTICLES, http://EzineArticles.com/4399575 (last updated Mar. 27, 2013).

[49] *Id*.

[50] *See Human Recognition Systems*, HUMAN RECOGNITION SYSTEMS, http://www.hrsid.com/vein-recognition (last viewed Oct. 17, 2012).

[51] *See Vein Recognition Biometrics*, FINDBIOMETRICS, http://www.findbiometrics.com/vein-recognition/ (last viewed Oct. 17, 2012).

[52] *See* Li Xueyan & Guo Shuxu, *The Fourth Biometric - Vein Recognition*, OPEN ACCESS DATABASE, http://cdn.intechopen.com/pdfs/5801/InTech-The_fourth_biometric_vein_recognition.pdf (last viewed 18 June 2013).

[53] *Id.*

[54] *Id.*

[55] CHUCK WILSON, VEIN PATTERN RECOGNITION: A PRIVACY-ENHANCING BIOMETRIC (Taylor & Francis Group/CRC Press, 2010).

vascular "bar" code reader for people.[56] Subcutaneous features can be conveniently imaged within the wrist, palm, and dorsal surfaces of the hand and further used for identification or verification. VPR technology functions through vein pattern infrared grey scale images that are binarized, compressed, and stored within in databases of two-dimensional vein images for comparison.[57] There are different types of vein recognition technology, which include finger vein, wrist vein, palm, and backhand vein recognition. The underlying concept of scanning remains the same with each of these techniques. VPR technology has extensive applications and can be applied to small personal biometric systems, such as a wrist watch like device termed a "Biowatch" or keys called "Biokeys" which emit unique identifier signals to access doors, locks or other secure environment.[58] Today, vein recognition biometric technology is most commonly found in the Asia-Pacific region, where it has found widespread acceptance. Japanese banks have adopted vein recognition across the country, where this kind of verification is becoming increasingly popular within the financial sector. One reason this new technology is being adopted so readily by banks is the fact that they are able to simply update their existing ATM software with the new Finger Vein Recognition[59] units, rather than installing brand new kiosks.[60]

Oftentimes, the new global interconnectedness also forces countries to alter or adapt their own national identification methods.

---

[56] *Id*.

[57] M. Rajalakshmi & R. Rengaraj, *Biometric Identification Using near Infrared Images of Palm Dorsal Vein Patterns*, INT'L J. ADVANCED ENGINEERING TECHNOLOGY (Oct.-Dec. 2011), *available at* http://www.technicaljournalsonline.com/ijeat/VOL%20II/IJAET%20VOL%20II%20ISSUE%20IV%20%20OCTBER%20DECEMBER%202011/ARTICLE%2063%20IJAET%20VOLII%20ISSUE%20IV%20OCT%20DEC%202011.pdf.

[58] JOHN R. VACCA, BIOMETRIC TECHNOLOGIES AND VERIFICATION SYSTEMS, 200 (2007).

[59] *See* Hitachi Corporation, *Finger Vein Authentication: White Paper*, *available at* http://www.hitachi.pl/veinid/documents/Finger_Vein_Authentication_White_Paper.pdf (last viewed June 18, 2013) (defining Finger vein recognition as: "…a new biometric method utilizing the vein patterns inside one's fingers for personal identity verification.").

[60] *See* McEwan, *supra* note 48.

For instance, as the U.S. incorporated biometric identifiers in U.S. visas, there was a mandate instituted which stated that similar technology was to also be used in foreign passports. The U.S., in the Enhanced Border Security and Visa Entry Reform Act of 2002,[61] required nations participating in the U.S. Visa Waiver Program to begin issuing new passports with biometric features supporting facial recognition.[62] The Visa Waiver Program allows travelers from twenty-seven countries to visit the U.S. for up to ninety days without a visa.[63] Travelers from countries participating in the U.S. Visa Waiver Program are required to enroll in identity verification and admissibility procedures.[64] The new U.S. travel requirements caused European governments to accelerate existing efforts toward the development of an integrated system of mutually recognized passports and national identity cards, both with embedded biometric identifiers.[65] As a result, in the last few years, biometric technology

---

[61] Enhanced Border Security and Visa Entry Reform, 8 U.S.C. §§ 1701-1778 (2004).

[62] *See* 18 U.S.C. § 1732 (c)(1) ("…the government of each country that is designated to participate in the visa waiver program … shall certify, as a condition for designation or continuation of that designation, that it has a program to issue to its nationals machine-readable passports that are tamper-resistant and incorporate biometric and document authentication identifiers that comply with applicable biometric and document identifying standards established by the International Civil Aviation Organization.").

[63] 18 U.S.C. § 1187, U.S. Dep't of State, *Visa Waiver Program (VWP)*, *available at* http://travel.state.gov/visa/temp/without/without_1990.html#2 (last visited Oct. 17, 2012) (giving the twenty-seven countries currently participating in the Visa Waiver Program: Andorra, Australia, Austria, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom).

[64] United States Visitor and Immigrant Status Indicator Technology Program, 8 C.F.R. §§ 215, 235, 252 (2011), *available at* http://www.setonresourcecenter.com/register/2009/jan/16/E9-988.pdf (last viewed Oct. 17, 2012). Enrollment for visa waiver countries is carried out at Electronic System for Travel Authorization. U.S. Customs and Border Protection, *Welcome to the Electronic System for Travel Authorization*, ELECTRONIC SYSTEMS FOR TRAVEL AUTHORIZATION, https://esta.cbp.dhs.gov/esta/ (last visited July 17, 2013).

[65] Thessaloniki European Council, *Presidency Conclusions*, 3 (Jun. 19 & 20, 2003), *available at* http://www.consilium.europa.eu/ueDocs/cms_Data/docs/

has been widely used to control international travel and continues to develop. In November 2005, Germany began issuing the first new biometric passports, which were valid for 10 years and included an embedded RFID (radio frequency identification) chip.[66] In the U.S., an automated immigration system using hand geometry is in the research and development phase within the Department of Homeland Security (DHS), which could eventually lead to a global traveler identification system.[67]

Biometrics is particularly popular in the context of law enforcement, dating back to the use of fingerprints and extending to its current reliance on DNA.[68] Although it has proven controversial in many ways, DNA identification is profiting from advances in technology that allow samples to filter very quickly through large databases in order to discern matches in minutes, as opposed to the days and sometimes weeks that it took when the technology was

---

pressData/en/ec/76279.pdf; ". . . [A] coherent approach is needed in the EU on biometric identifiers or biometric data, which would result in harmonized solutions for documents for third country nationals, EU citizens passports and information systems (VIS and SIS II). The European Council invites the Commission to prepare the appropriate proposals, starting with visas, while fully respecting the envisaged timetable for the introduction of the Schengen Information system II." *Id.*

[66] Dr. Gerrit Hornung, *The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards*, SCRIPT-ED (Volume 4, Issue 3, September 2007), *available at* http://www.law.ed.ac.uk/ahrc/SCRIPT-ed/vol4-3/hornung.pdf.

[67] *See* Jennifer Lee, *The Art and Craft of Security: Passports and Visas to Add High-Tech Identity Features*, N.Y. TIMES, Aug. 23, 2003, at 26 (explaining the fingerprinting and photographing procedures at ports of entry), *available at* http://www.nytimes.com/2003/08/24/us/art-craft-security-passports-visas-add-high-tech-identity-features.html?pagewanted=1viewed.

[68] For example, the FBI initially began using biometrics for identification in the 1920's in the form of fingerprinting. *See* Federal Bureau of Investigation, *Fingerprints and Other Biometrics*, FBI.GOV, *available at* http://www.fbi.gov/about-us/cjis/fingerprints_biometrics (last visited July 17, 2013). DNA profiling involves placing a numerical representation on the molecular sequences at DNA molecules at different points, called loci, which are then compared to other DNA profiles in a database. *See* Federal Bureau of Investigation, *The FBI and DNA*, FBI.GOV, *available at* http://www.fbi.gov/news/stories/2011/november/dna_112311 (last visited Oct. 18, 2013).

introduced.[69] Law enforcement in various countries, including Canada, Germany, and the U.S., already have some variation of a central DNA database or repository. Currently, in the U.S., every state, the District of Colombia, and the Federal Bureau of Investigation (F.B.I.), share DNA profiles through the Combined DNA Index System (CODIS).[70] Through CODIS, the F.B.I stores and manages DNA profiles in a National DNA Index System (NDIS) F.B.I. database which links to all federal and state programs.[71] CODIS contains DNA profiles collected from crime scenes, missing persons, unidentified human remains, and arrestees.[72] Compulsory DNA collection statutes have been challenged and upheld in both Federal and state courts.[73] In the U.S. as well as the United Kingdom (U.K.), law enforcement has utilized voluntary collection of DNA in targeted circumstances, particularly when faced with unsolved criminal activity in a particular area where DNA might exclude or include a particular individual. It is also true that those who refuse to offer a DNA sample have come under added scrutiny, making such request for a sample less than voluntary.[74]

---

[69] *See* Debra A. Herlica, *DNA Databanks: When Has a Good Thing Gone Too Far?*, 52 SYRACUSE L. REV. 951, 958 (2002); *See also* Scott N. Cameron, *Chapter 906: California's DNA Data Bank Joins the Modern Trend of Expansion*, 33 MCGEORGE L. REV. 219, 220 (2002) (reviewing the criticism and controversy surrounding DNA profiling). *See also* Sheryl H. Love, *Allowing New Technology to Erode Constitutional Protections: A Fourth Amendment Challenge to Non-Consensual DNA Testing of Prisoners*, 38 VILL. L. REV. 1617, 1632 (1993) (discussing the overbroad DNA testing of prisoners in American Prisons).

[70] Federal Bureau of Investigation - *Combined DNA Index System (CODIS)*, FBI.GOV, *available at* http://www.fbi.gov/about-us/lab/codis/ (last visited Oct. 12, 2012).

[71] U.S. v. Kincade, 379 F.3d 813, 819 (9th Cir. 2004) ("Today, over 170 public law enforcement laboratories participate in NDIS across the United States. Internationally, more than 40 law enforcement laboratories in over 25 countries use the CODIS software for their own database initiatives.").

[72] *Id.*

[73] *Id*. at 818-19 (noting that circuits are split between upholding the statutes based on totality of circumstances analysis and special needs. As of 2004 only two courts had invalidated DNA collection statutes: one district court and one state court later vacated on appeal).

[74] Bonnie L. Taylor, *Storing DNA Samples of Non-Convicted Persons & the Debate Over DNA Database Expansion*, 20 T.M. COOLEY L. REV. 509, 511

In the recent U.S. Supreme Case of *Maryland v. King*,[75] the Court held that when officers make an arrest supported by probable cause to hold a suspect for a serious offense and bring him to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment.[76] The Court stated that by comparison to the substantial government interest and the unique effectiveness of DNA identification, the intrusion of a cheek swab to obtain a DNA sample is minimal, and that reasonableness must be considered in the context of an individual's legitimate privacy expectations, which necessarily diminish when he is taken into police custody.[77] Justice Scalia filed a dissenting opinion in which Justice Ginsburg, Sotomayor, and Kagan joined. In the dissenting opinion Justice Scalia acknowledged that taking the DNA of arrested people could help solve more crimes and this "is a noble objective, but it occupies a lower place in the American pantheon of noble objectives than the protection of our people from suspicionless law-enforcement searches. The Fourth Amendment must prevail."[78]

B. Electronic Surveillance

In 1967, in his book *Privacy and Freedom*, Professor Alan Westin already warned about a "[d]eep concern over the preservation of privacy under the new pressures from surveillance technology."[79] Surveillance is a type of information collection that affects privacy and consists of monitoring and recording the movements of an

(2003).

[75] *Maryland v. King*, 569 U.S. __ (2013). The case was brought by Alonzo King, whose DNA was taken when he was arrested for allegedly waving a gun in public. After DNA analysis police determined that Alonzo's DNA matched that found in a six-year-old unsolved rape.

[76] *Id.* at 8-12.

[77] *Id.* at 23-24.

[78] *Id.* at 17.

[79] ALAN F. WESTIN, PRIVACY AND FREEDOM 330-64 (1970).

individual or group of individuals.[80] The term "electronic surveillance" refers to the use of electronic or mechanical devices to gather information about individuals' private communications and activities, primarily by law enforcement and governmental entities.[81] Abuses in electronic surveillance, what is also known as "wiretapping," have been revealed in many countries; often these have occurred on a very large scale with thousands of individuals subjected to illegal intercepts.[82] The targets of these intrusions have been such people as dissidents, opposition, human rights proponents, and student activists.[83] Such wide scale interceptions are possible because just about every country has established some level of wiretapping capacity over conventional wire communications such

---

[80] UK Home Office, COVERT SURVEILLANCE AND PROPERTY INTERFERENCE: REVISED CODE OF PRACTICE 7 (2010), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf.

[81] Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9 (2004) (providing an appropriate definition of "electronic surveillance").

[82] Revelations by whistleblower Edward Snowden made public that the US National Security Administration (NSA) engaged in a wide-ranging data mining project known as "Prism" to access a "vast quantity of emails, chat logs and other data directly from the servers of nine internet companies." Ian Black, *NSA Spying Scandal: What We Have Learned*, THE GUARDIAN (June 10, 2013), *available at* http://www.guardian.co.uk/world/2013/jun/10/nsa-spying-scandal-what-we-have-learned.

[83] It is important to recognize that governmental surveillance has not only been conducted by totalitarian governments. In fact, democratic governments in countries such as the United States have a dark history of governmental surveillance of civilians. *See* CHRISTOPHER H. PYLE, MILITARY SURVEILLANCE OF CIVILIAN POLITICS 1967-1970 (1986) (disclosing the military's surveillance of civilian politics. As a former captain in Army intelligence, he also recruited 125 former agents to tell what they knew about that spying to Congress, the courts, and the press. Those disclosures ended the Army's domestic spying and began a series of investigations into the misuse of intelligence agencies that historians now refer to as the Watergate era. Pyle worked on those investigations a consultant to Senator Sam J. Ervin's Subcommittee on Constitutional Rights and Senator Frank Church's Select Committee on Intelligence). *See* United States Department of State, *U.S. Department of State Country Report on Human Rights Practices 1997 – Singapore* (Jan. 30, 1998), *available at* http://www.unhcr.org/refworld/docid/3ae6aa1d18.html, for examples of governmental surveillance by other countries.

as telephone, telex, and fax.[84] Most commonly, the interceptions are overseen by law enforcement given their natural desire to obtain intelligence.[85] To further this objective, law enforcement has, out of necessity, forged very close relationships with the controllers of telecommunications, and through these affiliations has guaranteed, through mandatory software and hardware modifications, that telephony be "easily" wiretapped. These arrangements vary from permitting police direct physical access to telephone routing stations or exchanges, to hardwiring equipment to facilitate automatic interception.[86]

The U.S. has pushed extensively for a more concerted global campaign to enhance the capacity of law enforcement and intelligence entities to monitor electronic communications and conversations.[87] The effort has had two main components. The initial

---

[84] Incidentally, wiretapping did not start with the telephone. In the United States Civil War generals used telegraph wiretappers, as did stockbrokers in the 1860s. *See* SAMUEL DASH ET AL., THE EAVESDROPPERS 23 (1971) (1959). It was not until the early 1890s, that New York City police began to tap telephone lines for investigations. *See* WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 220-21 (2007). Early wiretaps consisted of connections made to the wires running to telephone or telegraph poles. Eventually, the technology evolved into the transmission of the tapped signal via an alternate line to a secure location for recording and monitoring. Steven Bellovin et al., *Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP*, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA 5 (2006), *available at* www.cs.columbia.edu/~smb/papers/CALEAVOIPreport.pdf.

[85] Private entities have also been ensnared in some eavesdropping scandals, as evidenced by Rupert Murdoch's News Group Newspapers who publicly acknowledged engaging in well-publicized phone and e-mail hacking scandal of victims of 9/11 attaches, celebrities and others, with some claims being settled in early 2012. Sarah Lyall & Ravo Somaiya, *Murdoch Settles Suits by Dozens of Victims of Hacking*, N.Y. TIMES, (Jan. 19, 2012), *available at http://www.nytimes.com/2012/01/20/world/europe/murdoch-company-settles-with-36-hacking-victims.html?pagewanted=all&_r=0*.

[86] *See* 47 U.S.C. §§ 1001-1010 (Communications Assistance for Law Enforcement Act) which requires telecommunications carriers to provide facilities "enabling the government, pursuant to a court order, to intercept all wire and electronic communications carried by the carrier."

[87] In 1994, The U.S. Congress passed the Communications Assistance for Law Enforcement Act (CALEA) to aid law enforcement in its effort to conduct

phase was to mandate that all existing telecommunications systems—telephone, satellite and mobile—and any new or emerging technologies have built-in surveillance access points; the second aspect of this strategy was to curtail the availability of encryption software that might allow for thwarting the first goal by preventing useful interception.[88] Technologically speaking, today it is relatively easy for governments to intercept and monitor individuals' communications; the only barriers to unfettered government monitoring are the legal protections available in most legal systems in the world. [89]

1. Video Surveillance and CCTV

Another modern development in the monitoring and recording of activities has been the use and deployment of cameras to conduct video surveillance throughout the world and often in public places. The technology[90] used in video surveillance has become very advanced.[91] Cameras can now be interconnected

---

criminal investigations requiring wiretapping of digital telephone networks. *Id.* The Act forces telephone companies to have the technology available to make it possible for law enforcement agencies to tap any phone conversations carried out over its networks, as well as making call detail records available. The act also provides that it must not be possible for a person to detect that his or her conversation is being monitored. *Id.*

[88] *See* DAVID GREISLER & RONALD J. STUPAK, HANDBOOK OF TECHNOLOGY MANAGEMENT IN PUBLIC ADMINISTRATION 597 (2006).

[89] Supplementing the Fourth Amendment, there are three primary federal statutes that serve to protect individuals' privacy in a network environment from wiretapping. Collectively known as the Electronic Communications Privacy Act (ECPA), the Stored Communications Act, the Wiretap Act, and the Pen Register statute regulate criminal investigators' access to both in-transit electronic communications and stored content, including emails stored with ISPs. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 (2004).

[90] The combined use of cameras and recording or projection devices for surveillance is often referred to by the acronym CCTV or Closed Circuit Television.

[91] Aimee Jodoi Lum, *Don't Smile, Your Image Has Just Been Recorded on a Camera-Phone: The Need for Privacy in the Public Sphere*, 27 U. HAW. L. REV.

systematically to form integrated networks that canvass not merely a few city blocks but large swathes of public space at once.[92] Cameras that capture images with high resolution can also be equipped with such enhancements as motion detection and infrared night vision capabilities.[93]Operators of the equipment can program the cameras so that the devices can automatically archive, track, and identify suspicious "behavior."[94] Technology continues to push ahead: the DHS is testing a program that would allow its agents to use cell phones and e-mail devices to record and share live video footage of suspected terrorists, and the French Interior Ministry has announced it will begin using flying drones outfitted with night-vision video cameras to monitor crime.[95]

Great Britain has made mass use of public Closed Circuit

377, 415 (2005) (advancing that statutory changes to keep up with modern technology usually in the form of camera-phones and very compact video cameras has facilitated voyeurism).

[92] *Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties*, THE CONSTITUTION PROJECT i, xi (2007), *available at* http://www.constitutionproject.org/manage/file/54.pdf [hereinafter THE CONSTITUTION PROJECT].

[93] Traditional wireless hotspots restricted access to relatively confined geographical areas. However, mesh networks—networks in which many wireless signals link together to form a blanket of coverage—have a farther reach. A Motorola mesh network, for instance, has girded the Los Angeles Police Department's video surveillance network at the notoriously crime-plagued Jordan Downs housing project. Mark Lacter, *Motorola's High-Speed Wireless Networks Give Cops Slick New Tools to Fight Crime*, FAST COMPANY (Nov. 1, 2007), *available at* http://www.fastcompany.com/magazine/120/wi-fi-meets-the-wire.html. Some developers of mesh network technology have said that public sector need for security wireless systems has fueled the domestic demand for their products. *See* Press Release, Firetide, Inc., Firetide Ablaze with Eight Consecutive Quarters of Record Revenue Growth (Oct. 23, 2007), http://www.firetide.com/innercontent.aspx?taxid=16&id=892; Rosie Lombardi, *Wi-Fi Growth Fuels Video Surveillance*, NETWORK WORLD (Oct. 29, 2007), http://www.networkworld.com/news/2007/102907-wi-fi-growth-fuels-video-surveillance.html.

[94] *See* THE CONSTITUTION PROJECT, *supra* note 92.

[95] Mimi Hall, *Surveillance System Raises Privacy Concerns*, USA TODAY (Feb. 28, 2008), http://www.usatoday.com/news/nation/2008-02-28-airvideo_N.htm; *France to Strengthen Video Surveillance System*, REUTERS (Oct. 12, 2007), http://www.reuters.com/article/inDepthNews/idUSL1272534220071012.

Television (CCTV) surveillance since around 1985.[96] A vast majority of cities and towns have implemented CCTV technology to monitor public spaces on an ever increasing scale.[97] Many central districts throughout the country are blanketed by CCTV, which operates within a concerted network of sophisticated cameras that have such features as infrared, panning, wide-angle and zoom. The latest addition to CCTV technology is CCTV microphones, which are highly sensitive microphones attached to public CCTV cameras.[98] The new generations of CCTV permit the recording of audio data as well as video data to give a more complete account of activities out in public, including conversations in public spaces. CCTV microphones can be triggered on the basis of decibel level or sound intensity, the speed at which words are spoken, and by certain words considered aggressive.[99] Although covertly recording private conversations could be deemed to be eavesdropping, it is only prohibited, without due authorization, in areas where privacy is reasonably expected.[100] Any expectation of privacy disappears when the audio recording is conducted in public and does not expressly

---

[96] In the U.K. alone, between 150 and 300 million pounds per year is now spent on a surveillance industry involving an estimated 200,000 cameras monitoring public spaces, or approximately 20% of all public monitoring cameras in the world. House of Lords, Science and Technology Committee, *Fifth Report, "Digital images as evidence,"* PARLIAMENT.UK (Feb. 3, 1998), *available at* http://www.parliament.the-stationery-office.co.uk/pa/ld199798/ldselect/ldsc tech/064v/st0501.htm.

[97] There are an estimated 4.2 million cameras in public spaces in Britain, around one for every fourteen individuals, which constitutes the highest concentration of such cameras in the world. *Report on the Surveillance Society*, SURVEILLANCE STUDIES NETWORK (Sept. 19, 2006), *available at* http:// www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf.

[98] *See* Gemma Simpson, *'Big Brother' cameras listen for fights*, CNET/NEWS, *available at* http://news.cnet.com/Big-Brother-cameras-listen-for-fights/2100-1029_3-6137888.html (last visited June 19, 2013).

[99] *Id* (explaining that in the U.K. and in the Netherlands CCTV cameras fitted with microphones listen for people speaking in aggressive tones).

[100] The European Court of Human Rights in *P.G. and J.H. v. The United Kingdom*, stated that CCTV cameras in public can be legitimately compared to the eyes of security guards. P.G. and JH v. The United Kingdom, no. 44787/98, 58, ECHR 2001-IX.

pertain to private matters.[101]

The use of cameras to monitor public spaces has also increased significantly in North America and other parts of the world.[102] In a growing number of U.S. cities, such as Manhattan and Washington D.C., there are now elaborate CCTV systems.[103] Beginning in 2003, Chicago deployed one of the most sophisticated networked systems, linking 1,500 cameras, placed by the city, to thousands more installed by public and private operators in trains, buses, public housing projects, schools, businesses, and elsewhere.[104] Homeland Security grants were used to fund the majority the project, referred to as Operation Virtual Shield. The system integrates the cameras with the emergency calling system and automatically feeds nearby video to the screen of an emergency services dispatcher after a 911 call.[105] In 2009, Mayor Richard Daley[106] said that he hoped to

---

[101] *See* Murray v Big Pictures Ltd, 3 WLR 1360 (2008). "As we see it, the question whether the reasonable expectation of privacy is a broad one, which takes account of all the circumstances of the case. They include the attributes of the claimant, the nature of the activity in which the claimant was engaged, the place at which it was happening, the nature and purpose of the intrusion, the absence of consent and whether it was known or could be inferred, the effect on the claimant and the circumstances in which and the purposes for which the information came into the hands of the publisher." *Id.*

[102] In the U.K., 90% of all schools had CCTV cameras, with an average of 24 cameras in each secondary school. Ben Quinn, *CCTV Cameras Being Used in School Changing Rooms and Toilets*, THE GUARDIAN (Sept. 11 2012), http://www.guardian.co.uk/world/2012/sep/11/cctv-cameras-school-changing-rooms; In the U.S., 70% have reported using CCTV according to a survey by the National Association of School Psychologists. *Research on School Security*, NASP, http://www.nasponline.org/advocacy/schoolsecurity.pdf (last visited Jun. 13, 2013).

[103] Robert N. Strassfeld & Cheryl Ough, *Somebody's Watching Me: Surveillance and Privacy in an Age of National Insecurity*, 42 CASE W. RES. J. INT'L L. 543, 543 (2010).

[104] William M. Buckley, *Chicago's Camera Network is Everywhere*, WALL ST. J. (Nov. 17, 2009), *available at* http://online.wsj.com/article/SB10001424052748704538404574539910412824756.html; Fran Spielman, *Eyes Everywhere: City Wants Businesses, Residents to Share Surveillance Video*, CHI. SUN TIMES (July 24, 2008).

[105] Press Office of the Mayor of Chicago, *Mayor Daley Announces Major Upgrade to Chicago's 911 System*, CITYOFCHICAGO.ORG (Feb. 19, 2009), http://mayor.cityofchicago.org/mayor/en/press_room/press_releases/2009/february_2009

have a camera on every street corner by 2016.[107] More recently, New York City announced the Lower Manhattan Security Initiative,[108] based on London's experience with CCTV systems.[109]

For the most part, there is precious little regulation of the deployment and use of cameras to survey public spaces in general.[110] In Europe, although Directive 95/46/EC[111] covers both audio and video data, there is no comprehensive framework for regulating the latest and ongoing enhancements to public CCTV surveillance capabilities. In the U.S., the lack of regulation regarding CCTV technology results from the policy that under U.S. law, a public place is generally considered to be one in which individuals do not have a reasonable expectation of privacy.[112] Consequently, what occurs in

/mayor_daley_announces.htmlviewed.

[106] Andrew Stevens, *Richard M Daley former Mayor of Chicago*, CITY MAYORS, http://www.citymayors.com/mayors/chicago_mayor.html (last visited June 4, 2013) (explaining that Mayor Richard Daley is the former Mayor of Chicago, IL., from 1989 until 2011).

[107] Fran Spielman, *Surveillance Cams Help Fight Crime, City Says; Goal Is to Have Them on Every Corner*, CHI. SUN TIMES Feb. 20, 2009, at 22.

[108] According the City of New York the Lower Manhattan Security Initiative is [an] "integrated approach to security consists of an increased presence of uniformed officers on the streets, and the use of counterterrorism technologies … deployed in public areas, including closed circuit televisions owned by the NYPD and its various private and public partners, license plate readers, and chemical, biological, radiological, and nuclear detector." New York City Police Department, *New York City Police Department Releases Draft of Public Security Privacy Guidelines for Public Comment*, NYC.GOV (FEB. 25, 2009), http://www.nyc.gov/html/nypd/html/pr/pr_2009_005.shtml.

[109] Michael Howard Saul, *Bloomberg to Study London's "Ring of Steel,"* WALL ST. J., May 10, 2010, at A21.

[110] Thomas D. Colbridge, *Electronic Surveillance: A Matter of Necessity*, FBI L. ENFORCEMENT BULL. 26, (February 2000), *available at* http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2000-pdfs/feb00leb.pdf.

[111] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31, *available at* https://www.cdt.org/privacy/eudirective/EU_Directive_.html (last visited Oct. 26, 2012).

[112] *See* Katz v. United States, 389 U.S. 347 (1967) (involving a reputed bookmaker using a public telephone booth to communicate about illegal gambling. Unbeknownst to Katz, the FBI was recording his conversations by use of an

public spaces cannot be safeguarded as a private activity and courts have not imposed constraints on the use of CCTV. Recently, some have begun to argue that the technology for public surveillance is so advanced and its use is so pervasive that there needs to be some type of regulation to protect individual privacy.[113]

2. Unmanned Aerial Systems (Drones)

Most of us are familiar with unmanned aerial systems (UAS),[114] more commonly known as "Drones" from their use in such places as Afghanistan, Pakistan and Yemen.[115] The Federal Aviation Administration (FAA) develops procedures to allow commercial and public UAS.[116] In addition to the term "drone," these types of crafts

---

electronic device connected to the exterior of the telephone booth without a physical intrusion of the interior space. The Court held that the Government's activities which involved electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment. The Court held that a conversation is protected from unreasonable search and seizure under the Fourth Amendment if it is made with a "reasonable expectation of privacy).

[113] Jeremy Brown, *Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places*, 23 BERKELEY TECH. L.J. 755 (2008).

[114] "Unmanned aerial vehicles commonly referred to as UAV's [or drones] are defined as powered aerial vehicles sustained in flight by aerodynamic lift over most of their flight path and guided without an onboard crew." *Introduction of the Unmanned Aerial Vehicles*, U.S. DEP'T OF DEFENSE, http://www.defense.gov/specials/uav2002/ (last visited July 18, 2013).

[115] Declan Walsh & Eric Schmitt, *Drone Strike Killed No. 2 in Al Qaeda, U.S. Officials Say*, N.Y. TIMES (June 5, 2012), *available at* http://www.nytimes.com/2012/06/06/world/asia/qaeda-deputy-killed-in-drone-strike-in-pakistan.html?pagewanted=all; *US Drone Strike Kills Five Insurgents Near Afghan Border*, THE TELEGRAPH (Oct. 10, 2012), http://www.telegraph.co.uk/news/worldnews/asia/pakistan/9597737/US-drone-strike-kills-five-insurgents-near-Afghan-border.html#; *Anwar al-Awlaki: Drone Kills US-born Preacher Who Inspired Lone Wolf Terrorists*, THE TELEGRAPH (Sept. 30, 2011), *available at* http://www.telegraph.co.uk/news/worldnews/al-qaeda/8800346/Anwar-al-Awlaki-Drone-kills-US-born-preacher-who-inspired-lone-wolf-terrorists.html.

[116] *See FAA Notice on Unmanned Aircraft Systems (UAS)*, FAA (Jan. 22,

may also be referred to as "unmanned aircrafts," "remotely piloted aircrafts," or "unmanned aerial vehicles." The main characteristics of UAS are that they do not carry a pilot onboard, but function from "pilot" control from the ground or elsewhere, and they use pre-programmed flight coordinates. The first known public mention of UAS dates back to around 1915 in the works and writings of Serbian-American inventor and engineer Nikola Tesla who theorized about flying machines that could be radio controlled.[117]

It was not until the beginning of the Cold War that UAS truly began to show their usefulness as a reconnaissance tool.[118] Over time, they have evolved into being used for three categories of action: as attack weapons, as operation or strike tools, and as surveillance or reconnaissance systems.[119] All the functioning of the UAS is generally controlled via a laptop computer, a kit mounted on a vehicle, or in a larger fixed facility.[120] The current military inventory for unmanned aerial vehicles exceeds 6,000 spread out among all branches of the military, with significant increases planned in the future.[121]

The use of UAS have many advantages for the military, such as low costs, both for flying as well as maintenance and acquisition, longer flight times, and less risks to pilots. Such advantages have also made UAS very attractive to the law enforcement and civilian

---

2013), http://www.faa.gov/documentlibrary/media/notice/n%208900.207.pdf.

[117] *Tesla's (real) Flying Machine*, *available at* http://www.pritchardschool.com/Teslas_Flying_Machine.pdf, (last visited Oct. 17, 2012); Martin E. Dempsey, *Eyes of the Army – U.S. Army Roadmap for Unmanned Aircraft Systems* 2010–2035, UNITED STATES ARMY (Apr. 9, 2010), *available at* http://www-rucker.army.mil/usaace/uas/US%20Army%20UAS%20RoadMap%202010%202035.pdf.

[118] *See* Rajesh Kumar, Sqn Ldr, *Tactical Reconnaissance: UAVS Versus Manned Aircraft*, 1 (March 1997), available at http://www.fas.org/irp/program/collect/docs/97-0349.pdf.

[119] *See* Dempsey, *supra* note 117, at 3-4.

[120] *Id.*

[121] Report to Congressional Committee, *Report on Future Unmanned Aerial Systems Training, Operations, and Sustainability*, UNITED STATES AIR FORCE (Sept. 2011), http://www.fas.org/irp/program/collect/uas-future.pdf.

markets.[122] The FAA regulates the use of drones and grants licenses on a case-by-case basis after determining the "airworthiness" of the system.[123] As stated in the Government Accountability Office report ("GAO report"), the authorized uses are limited to "activities such as law enforcement, search and rescue, forensic photography, monitoring or fighting forest fires, border security, weather research, and scientific data collection."[124] The GAO report goes on to state that the ultimate goal for the FAA is to expand unmanned aviation to the "greatest extent possible."[125]

Privacy concerns, regarding unmanned aerial vehicles, center on the fact that these vehicles provide almost limitless access to view and record events from the sky, without the consent or knowledge of those being surveyed.[126] It is easy to imagine how this technology could be abused. In the only reported U.S. court case involving a challenge to the use of a surveillance drone, a North Dakota man challenged the use of such an aircraft that was used by law enforcement to conduct surveillance of his private property.[127] The Court concluded that "'there was no improper use of an unmanned

---

[122] "Domestically, state and local law enforcement entities represent the greatest potential users of small UAS in the near term because they can offer a simple and cost effective solution for airborne law enforcement activities." *UNMANNED AIRCRAFT SYSTEMS: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System*, REPORT OF THE GOVERNMENT ACCOUNTABILITY OFFICE (Sept. 2012), *available at* http://www.gao.gov/assets/650/648348.pdf [hereinafter *UNMANNED AIRCRAFT SYSTEMS*].

[123] From January 1, 2012, and July 13, 2012, "FAA issued 342 COAs to 106 federal, state, and local government entities across the United States, including law enforcement entities as well as academic institutions. Over the same time period, FAA issued 8 special airworthiness certifications for experimental use to four UAS manufacturers." *Id.* at 11.

[124] *UNMANNED AIRCRAFT SYSTEMS*, *supra* note 122, at 49.

[125] *Id.*

[126] *See* Eric Posner, *The Killer Robot War Is Coming: The new laws we need to govern the use of drones*, SLATE (May 15, 2013), *available at* http://www.slate.com/articles/news_and_politics/view_from_chicago/2013/05/drone_warfare_and_spying_we_need_new_laws.html.

[127] Order Denying Motion to Dismiss, No. 32-2011-CR-00049, (N.D. Nelson Cty. Dist. Ct. July 31, 2012), http://www.nacdl.org/uploadedFiles/files/news_and_the_champion/DDIC/Brossart%20Order.pdf.

aerial vehicle' because the drone 'appears to have had no bearing on these charges being contested here. . .'"[128] Although the Court did not directly address the privacy issues involved in the use of the drones, and the case was decided on other grounds, it is a precursor of some of the issues that are likely to be raised regarding UAS's surveillance.[129]

3. Internet Surveillance

The explosion in the availability and access to the Internet has made it one of the principal tools for communication, commerce, and research. With the hyper-development of new technologies and applications, the Internet is constantly evolving; with it have blossomed new and ever more creative uses for the World Wide Web.[130] Not only are the uses of the Internet extraordinary, so is its growth. The worldwide number of Internet users surpassed 2.4 billion in 2012—up from only approximately 1.2 million in 2006.[131] However, because of its relative youth in mass application, the Internet lacks many of the protections and control mechanisms utilized for systems like hard wired telephony. Such things as the unauthorized collection and storage of information relating to Internet activities have emerged as significant threats to privacy on the Internet.[132] With each keystroke and page that is opened, data

---

[128] Jason Koebler, *Court Upholds Domestic Drone Use in Arrest of American Citizen*, US NEWS & WORLD REPORTS (Aug. 2, 2012), http://www.usnews.com/news/articles/2012/08/02/court-upholds-domestic-drone-use-in-arrest-of-american-citizen.

[129] State of North Dakota vs. Rodney Brossart, No. 32-2011-CR-00049 (D. N.D. 2012 Aug. 1, 2012) (order denying motion to dismiss).

[130] Robert A. Pikowsky, *Legal and Technological Issues Surrounding Privacy of Attorney Client Communications Via Email*, 43 ADVOCATE 16 (2000).

[131] *See World Internet Users Statistics Usage and World Population Stats*, INTERNET WORLD STATS (June 30, 2012), http://www.internetworldstats.com/stats.htm; *Worldwide Internet Users Will Top 1.2 Billion in 2006*, COMPUTER INDUSTRY ALMANAC, INC. (Feb. 12, 2007), http://www.c-i-a.com/pr0207.htm.

[132] Ric Simmons, *Technological Change and the Evolution of Criminal Law: Why 2007 is Not Like 1984: A Broader Perspective on Technology's Effect on*

servers collect, store and catalog very precise information about the user and his or her use of the Internet. Many sites utilize what are commonly known as "cookies,"[133] which are placed on an Internet users' access device and facilitates detailed information about the user, often without the user's knowledge or consent. Adding to the amount of personal data collected are the websites that require personal data before use; there are also others that obtain information in connection with purchases, all of which are readily vulnerable to theft and abuse. Other sites such as Google, Twitter, Facebook, Instagram and LinkedIn, accumulate personal data of users with alarming specificity.[134] They are able to know such things as where individuals log on from, their use patterns and their personal and professional personal contacts.[135] The collection and retention of this data is a source of great concern and has also been sought by governments and others for non-commercial purposes, such as academic institutions, non-governmental entities, political parties and others.

With the potential for data mining, governments have also rushed full speed into internet surveillance. National governments have in many instances begun filtering and monitoring the Internet

---

Privacy and Fourth Amendment Jurisprudence, 97 J. CRIM. L. & CRIMINOLOGY 531, 533 (2007) (the author discusses the effect of technology on Fourth Amendment cases and argues for an appropriate balance between an individual's right to privacy and the government's interest in law enforcement); *see* Meir S. Hornung, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 118 (2005) (discussing privacy interests in the workplace regarding e-mail communications).

[133] "A *cookie* is a small amount of data generated by a website and saved by your web browser. Its purpose is to remember information about you, similar to a preference file created by a software application." *Cookie Definition*, TECHTERMS.COM, http://www.techterms.com/definition/cookie (last visited June 13, 2013).

[134] A well-known example is Google's Flu Trends report that is based on the geographical locations associated with IP addresses of individuals entering queries that Google assumes reflect a local case of the flu. *Explore flu trends around the* world, GOOGLE.org, http://www.google.org/flutrends/ (last visited June 20, 2013).

[135] Dan Jerker B. Svantesson, *Geo-Location Technologies and Other Means of Placing Borders on the "Borderless" Internet*, 23 J. MARSHALL J. COMPUTER & INFO L. 101, 109-10 (2004) (describing how geolocational services can build databases to identify the location associated with IP addresses).

for criminal, amoral, or political activities.[136] In particular, authoritarian or repressive regimes, such as China, Cuba, and Iran, have attempted to exercise almost complete control over access to the Internet.[137] The most common way this is accomplished is by controlling the Internet Service Providers (ISPs) that supply Internet access domestically. Utilizing these controls, governments can then very easily control, monitor and filter internet access. These regimes have gone so far as to "[shut] . . . down their communications grids to deny opponents the ability to coordinate in real time and broadcast documentations of an event."[138]

China is perhaps one of the best known instances of government surveillance of the Internet.[139] By the turn of the millennium, China was said to have been developing a program known as the "Golden Shield," described as "a gigantic online database with an all encompassing surveillance network incorporating speech and face recognition, closed-circuit television, smart cards, credit records, and Internet surveillance technologies."[140] Today, according to a variety of sources, the

---

[136] Revelations about the National Security Agency's Prism program for collecting vast amounts of electronic communications has highlighted the governmental use of and ability to conduct wide-scale data mining. Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 7, 2013), http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data.

[137] According to the internet watchdog group Freedom House, China, Cuba and Iran have the most restrictive internet filters in place. Sanja Kelley, et al., *Freedom on the Internet 2012*, FREEDOM HOUSE, http://www.freedomhouse.org/sites/default/files/FOTN%202012%20FINAL.pdf (last visited June 19, 2013).

[138] Clay Shirky, *The Political Power of Social Media Technology, the Public Sphere, and Political Change, Foreign Affairs*, FOREIGN AFF. 10 (Jan./Feb. 2011), *available at* http://www.yuswohady.com/wp-content/uploads/2011/01/The-Political-Power-of-Social-Media-Clay-Sirky-Foreign-Affairs.pdf.

[139] As Clay Shirky writes: "[t]he Chinese system has evolved from a relatively simple filter of incoming Internet traffic in the mid-1990s to a sophisticated operation that not only limits outside information but also uses arguments about nationalism and public morals to encourage operators of Chinese Web services to censor their users and users to censor themselves." *Id.*

[140] Greg Walton, *China's golden shield: corporations and the development of surveillance technology in the People's Republic of China*, *in* INTERNATIONAL

Chinese government is rumored to employ as many as 30,000 "cyber police" to provide near constant surveillance of blogs, forums, chats and internet search engines.[141] It is unknown to what extent other governments conduct internet surveillance.

4. Global Positioning System (GPS)

Another area of technology that is of concern when it comes to privacy is Global Positioning System (GPS) technology. To most people, a GPS is a tool that aids in finding directions or in locating friends and family on twitter or Facebook. GPS was first unveiled under the auspices of the U.S. Department of Defense around 1973; it stemmed from research that was then underway using satellite navigation for military uses.[142] Today, GPS technology is found in any number of devices including cellular telephones, "smart" phones, computers, laptops, computer tablets and vehicles of every type. The proliferation of this technology is in part due to the decreasing cost of the devices as well as the rapid advances in the technologies associated with the devices that can either track position or emit signals that can then be tracked.

The first mass use for GPS technology was in the area of transportation.[143] In the transportation sector, GPS gained widespread civilian use around 1996 when the military began to allow greater access to its satellites for civilian purposes.[144] Vehicles

---

CENTER FOR RIGHTS AND DEMOCRACY, 39 (2001), *available at* http://www.dd-rd.ca/site/_PDF/publications/globalization/CGS_ENG.PDF.

[141] James A. Lewis, *The Architecture of Control: Internet Surveillance in China*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (July 2006), *available at* http://csis.org/files/media/csis/pubs/0706_cn_surveillance_and_information_technology.pdf.

[142] NATIONAL RESEARCH COUNCIL, THE GLOBAL POSITIONING SYSTEM: A SHARED NATIONAL ASSET: RECOMMENDATIONS FOR TECHNICAL IMPROVEMENTS AND ENHANCEMENTS 16 (1995).

[143] *Id*.

[144] In 1995, President Bill Clinton in a policy directive stated that a national policy was "needed to balance commercial and civil uses of GPS with the essential national security aspects of the system…" *See Global Positioning System (GPS) Policy Review, PRD/NSTC-3[18 May 1995]*, THE WHITE HOUSE OFFICE OF MEDIA

were equipped with either fixed or removable devices that could be located or pinpointed to a location with great accuracy and then triangulate mapping information on a real time basis utilizing GPS technology. However, it became quickly apparent this technology had the corresponding ability of tracking the movements of those vehicles equipped with the devices. It did not take long for governments and others to see the surveillance value of such a technology for tracking the movements of individuals.[145]

As this technology has spread beyond vehicles and some of the more predictable applications, GPS technology has found its way into cyberspace. Social media networking sites, such as Facebook, are now using GPS receivers to allow their users to physically locate other users via "geolocation." One way geolocation is used is when a social media network site tracks a user's location based on where a photograph is taken. Twitter and Facebook, among others, also retain geolocators and other data imbedded in digital photographs that allow determination of where a photograph was taken. [146] Another example is Facebook's "Places" application, which utilizes geolocation to permit its users to "check in" and register their current location for all other users to see.

The search engine Google has integrated geolocation into its

AFFAIRS (June 2, 1995), *available at* http://www.fas.org/irp/offdocs/prd-nstc3.htm.

[145] The United States Supreme Court in a landmark decision in *U.S. v. Jones*, 10 U.S. 1259 (2012), decided in January 2012, limited police ability to track suspects using GPS device. The Supreme Court held that attaching a GPS device to a vehicle and then using the device to monitor the vehicle's movements constitutes a search under the Fourth Amendment. As a result of the breach, the Court held that the defendant's conviction for drug trafficking must be reversed when some of the evidence to convict him was obtained through a GPS tracking device on his car, because the attachment of the GPS tracking device and then the use of that device to monitor the car's whereabouts is a "search" for purposes of the Fourth Amendment. *Id.*

[146] A *New York Times* article recalls the surprise of Adam Savage, host of the US television program "MythBusters," who posted a picture on Twitter of his automobile parked in front of his house only to find that coding in the picture allowed anyone to find out where it was taken and, hence where he lived. Kate Murphy, *Web Photos That Reveal Secrets, Like Where You Live*, N.Y. TIMES (Aug. 11, 2011), *available at* http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html?pagewanted=all.

"Adwords"[147] advertising so that advertisers can get detailed information about the location of users.[148] Twitter also employs geolocation by allowing users to constantly broadcast, or "tweet," their thoughts and whereabouts in short messages from their computers, any web browser, or mobile phones. As this technology continues to evolve, scenarios not yet conceived will continue to concern privacy advocates.[149]

5. Radio Frequency Identification (RFID)

The newest, and probably most intrusive, technology that could be used for surveillance purposes is the implant of Radio Frequency Identification (RFID)[150] devices. The use of RFID

---

[147] Google Adwords is a marketing tool incorporated into Google's search engine wherein ads appear along with relevant content for the particular search.

[148] In fact, Google has taken the tracking of advertisers beyond just location through its use of Google Analytics, which involves an imbedded code in a website that provides detailed information about site visits to advertisers. These include IP addresses, length of search, entry and exit pages, as well as locations. An IP address is a code made up of numbers separated by three dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses may be static, which are always the same, or dynamic, which change each time you go on the internet. *IP Address* Definition, TECHTERMS.COM, *available at* http://www.techterms.com/definition/ipaddress (last visited June 19, 2013).

[149] A bill introduced in the June 2011 legislative session of the US Senate known as the "Relocation Privacy and Surveillance Act" (also known as the GPS Act) would require probable cause and an accompanying warrant before government agencies could obtain private geolocational information on an individual. Geolocational Privacy and Surveillance Act, S. 1212, 112th Cong. (2011-2012), *available at* http://wyden.senate.gov/download/?id=8af5e30b-950f-4af4-9b6a-7c76bb1f1167. The bill would also make it illegal for private businesses to share customer location data without explicit consent. The bill would cover real-time tracking data as well as previously acquired historical location data. *Id.*

[150] "Stands for 'Radio-Frequency Identification.' RFID is a system used to track objects, people, or animals using tags that respond to radio waves. RFID tags are integrated circuits that include a small antenna. They are typically small enough that they are not easily noticeable and therefore can be placed on many types of objects." *RFID* Definition, TECHTERMS.COM, http://www.techterms.com/definition/rfid (last visited June 19, 2013).

technology had its origins during World War II as a means to identify approaching aircrafts, and to determine whether they were friendly or enemy aircrafts.[151] RFID technology continued evolving until the 1980's, when prices began to fall allowing government and private entities to develop more expansive uses of the technology.[152] As RFID technology has become commercially viable within the last few years, it has developed into a functional replacement for the UPC barcode system.[153] In today's environment, RFID technology is primarily used commercially to allow for fast and reliable exchange of information from an RFID tag to an RFID reader in order to identify objects in the supply chain.[154] Like many emerging technologies, RFID technology showed early potential to provide great economic benefits for the government, businesses, and consumers, while at the same time posing a potentially serious threat to consumer privacy and personal security.

There are two categories of RFID tags in use: active and passive.[155] Active tags have a battery on the tag,[156] "which may be used to boost read/write range, allow for larger memories, or add sensory and data logging capabilities."[157] "Passive tags receive all of their energy from the read/write device that 'powers' the tag to allow it to transmit data."[158] High-volume applications almost exclusively use passive tags. In practice, the passive tag is attached to an item as

---

[151] DAN MULLEN & BERT MOORE, AUTOMATIC IDENTIFICATION AND DATA COLLECTION: WHAT THE FUTURE HOLDS, IN RFID APPLICATIONS, SECURITY, AND PRIVACY 3, 5 (Simson Garfinkel & Beth Rosenberg eds., Addison Wesley 2005).

[152] *See* Katherine Delaney, Note, *2004 RFID: Privacy Year in Review: America's Privacy Laws Fall Short with RFID Regulation*, 1 ISJLP 543, 548 (2005).

[153] UPC stands for Universal Product Code, and it is the standard scannable barcode, which is printed or affixed on nearly all retail products. *See* UPC HOME PAGE, http://www.upccode.net/faq.html (last visited Oct. 17, 2012).

[154] Charles J. Condon, *RFID and Privacy: A Look at Where the Chips are Falling*, 11 APPALACHIAN J. L. 101 (2011).

[155] *See RFID Solution Center, RFID FAQs, RFID Tag Characteristics*, ZEBRA TECHNOLOGIES, http://www.zebra.com/us/en/solutions/getting-started/rfid-printing-encoding/rfid-tag-characteristics.html (last visited Oct. 17, 2012).

[156] *Id.*

[157] *Id.*

[158] *Id.*

a unique identifier of that specific item. Detailed information about the item is encoded to the attached tag and automatically transmitted to a reads ad then records when the tag is activated and within range. A typical system can read the RFID tags at distances from 6 to 8 inches and up to 20 feet or more.[159] One of the key factors in any distribution system is the ability to keep track of products and materials, and establish procedures to ensure the quick and efficient delivery of shipments. The introduction of RFID technology in the area of global supply management was designed to increase operational efficiency by tagging individual boxes, shipping containers, or pallets with RFID tags that are capable of transmitting their unique identifying number to a strategically located RFID reader in the distribution network.[160] As containers are loaded onto trucks or railroad cars, the RFID reader automatically captures the identifier and records the location of each container. Although the containers are frequently loaded and unloaded in the normal course of distribution, the unique RFID tag in each container makes the status and location of each shipment ascertainable. Most major companies today use RFID technology for the purpose for which it was created; as an effective way of inventory control.[161] However, as inventory control components, RFID tags have universal appeal in other fields, such as: in the medical community to track medicines,[162]

---

[159] *Id.*

[160] *See* Claire Swedberg, *Auchan Track Produce Containers Via RFID*, RFID JOURNAL, *available at* http://www.rfidjournal.com/article/view/8933 (visited Oct. 17, 2012).

[161] Wal-Mart was an early adopter of RFID technology. When the concept of using RFID in distribution systems was initially introduced to industry, Wal-Mart recognized its potential almost immediately. *See* Bob Violino, *Wal-Mart Details EPC Rollout Plan*, RFID JOURNAL (June 17, 2004), http://www.rfidjournal.com/article/articleprint/992/-1/1/; *see also* Jonathan Collins, *IBM Expands RFID Services*, RFID JOURNAL (Sept. 14, 2004), http://www.rfidjournal.com/article/articleprint/1117/-1/1/.

[162] *Global Radio Frequency Identification (RFID) in Healthcare Industry is Expected to Reach USD 3,351.6 Million by 2018*, TRANSPARENCY MARKET RESEARCH, *available at* http://www.prnewswire.com/news-releases/global-radio-frequency-identification-rfid-in-healthcare-industry-is-expected-to-reach-usd-33516-million-by-2018-transparency-market-research-173257111.html (last visited Aug. 8, 2013).

equipment, and cadavers donated to science;[163] in the art community to track museum pieces;[164] in libraries to track books;[165] in the Justice system to track criminal case files;[166] and in the airline industry to track luggage.[167]

Recently, there has been a great deal of public discussion regarding RFID technology in the context of RFID human implants and for its potential as a privacy invading technology.[168] An RFID implant is an encapsulated RFID microchip that can be injected into human tissue.[169] A low frequency signal, 125-134 KHz, is emitted by an RFID reader, which remotely activates an RFID implant causing it to transmit its unique identification number back to the RFID reader. The microchip's unique ID number can be used to identify an individual and to access his/her stored personal information on an associated database, such as medical and information or biometric data. [170] RFID implants are FDA approved.[171]

---

[163] Michelle Locke, *Tracking Bodies Donated to Science*, CBS NEWS (Feb. 11, 2009), http://www.cbsnews.com/stories/2005/02/04/tech/main671872.shtml.

[164] Farat Khan, *Museum Puts Tags on Stuffed Birds*, RFID JOURNAL (Apr. 22, 2004), http://www.rfidjournal.com/article/view/1110.

[165] *See* Simon Edwards & Mike Fortune, A GUIDE RFID IN LIBRARIES (2008), *available at* http://www.bic.org.uk/files/pdfs/090109%20library %20guide% 20final%20rev.pdf; Elena Engel, *RFID Implementation in California Libraries: Costs and Benefits*, U.S. INSTITUTE OF MUSEUM AND LIBRARY SERVICES 20 (July 2006); David Dorman, *Technically Speaking: RFID Poses No Problem for Patron Privacy*, AMERICAN LIBRARIES (Dec. 2003).

[166] *See Circuit Locates Case Files in Real Time Using RFID*, ZEBRA TECHNOLOGIES, *available at* http://www.zebra.com/gb/en/solutions/research-and-learn/success-stories/florida-state-attorney.html (last visited Oct. 17, 2012).

[167] *Airlines Tagging Luggage with RFID*, RFID GAZETTE (Feb. 14, 2005), *available at* http://www.rfidgazette.org/2005/02/airlines_taggin.html.

[168] W.A. Herbert, *No Direction Home: Will the Law Keep Pace With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?* 2(2) JLPIS 409 (2006).

[169] *See generally* Elaine M. Ramesh, *Time Enough? Consequences of Human Microchip Implantation*, 8 RISK 373, 378 (1997) (describing the forms of implantable microchips). A read-write microchip "would be capable of carrying a set of information which could be expanded as necessary." *Id.* A read-write and tracking microchip would have all the capabilities of a read-write microchip, as well as the ability to "emit a radio signal which could be tracked." *Id.*

[170] Jonathan Collins, *Tracking Medical Emergencies*, RFID JOURNAL (APR.

The VeriChip Corporation (VeriChip) established itself as the frontrunner in the arena of manufacturing RFID implants, tracing its origination back to September 11, 2001, "when New York firemen were writing their badge ID numbers on their chests in case they were found injured or unconscious."[172] Roughly three years after its creation, VeriChip received FDA approval for its human-implantable microchip in medical applications, and it is currently the only company in the world offering an FDA-approved microchip.[173] VeriChip reports a sale of 7,000 microchips worldwide, 2,000 of which have been implanted in humans.[174] Currently, most of VeriChip's sales have occurred internationally.[175] For instance, the Attorney General of Mexico and members of his staff use the microchip as a security pass to access secured areas.[176] The company has broadened its market, and today's implantation of RFID's also takes place in high-risk patients, particularly in individuals with diabetes or Alzheimer's disease.[177]

Critics of RFID technology, regarding tagging of consumer information, argue the benefits of company utility and consumer

---

22, 2004), http://www.rfidjournal.com/article/view/901 (noting that a "tag was attached to an ankle of arriving patients as soon as they entered the center").

[171] *See* Laurie Barclay, M.D., *FDA Approves Implantable Chip Used to Access Medical Records*, MEDSCAPE TODAY, http://www.medscape.com/viewarticle/491994 (last visited Oct. 17, 2012).

[172] *See VeriChip Corporation, Company Profile*, POSITIVE ID, http://www.positiveidcorp.com/investors_prm.html (last visited Oct. 17, 2012).

[173] *Id.*

[174] Michael Kanellos, *Microchips in Humans*, C/NET (Aug. 23, 2004) http://news.cnet.com/human-chips-more-than-skin-deep/2009-1008_3-5318076.html.

[175] *Id.*

[176] *See* Will Weissert, *Microchips Implanted in Mexican Officials*, MSNBC.COM (July 14, 2004), *available at* http://www.msnbc.msn.com/id/5439055/ns/technology_and_science-tech_and_gadgets/t/microchips-implanted-mexican-officials/.

[177] *See* Adam Frucci, *RFID Microchips Implanted into Alzheimer's Patients*, GIZMODO (Aug. 29, 2007), http://gizmodo.com/294731/rfid-microchips-implanted-into-alzheimers-patients; Lance Laytner, *Verichip to Implant Alzheimer's Patients*, MERITUM MEDIA (Nov. 3, 2008), http://www.meritummedia.com/health/verichip-to-implant-alzheimers-patients.

convenience do not outweigh the costs of infringement on privacy rights when personally identifiable information is linked to data collected by RFID systems.[178] They argue that RFID tags in passports, credit cards, baggage, library books, and various other consumer products could become tracking devices where retailers, law enforcement, and other unauthorized individuals could track persons simply by installing nearby readers.[179] To avoid this danger, many consumer groups are advocating for strict regulations or complete bans on RFID technology.[180] So far, most legislation addressing RFID technology is related to the use of RFID embedded in consumer products or identity documents.[181] The argument is that RFID legislation regarding data tagging needs to be consistent and protective of consumers' rights.[182] Critics of RFID implants in humans cite the potential as a privacy-invading technology based on the lack of legislation for the regulation of the technology.[183] Although there are some existing US State laws on RFID, they vary on substance. Some states have adopted legislation that prohibits the forced or involuntary placing of RFID implants; however, most states have not addressed the ethical or privacy implications of voluntary RFID human implants.[184] In the European Union, the issue

---

[178] *See* Serena G. Stein, *Where will Consumers Find Privacy Protection from RFID's?: A Case for Federal Legislation*, 2007 DUKE L. & TECH. REV. 3 (March 2007).

[179] *See Radio Frequency Identification (RFID) Systems*, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/privacy/rfid (last visited Oct. 17, 2012).

[180] *Opponents of RFID include: Consumers Against Supermarket Privacy Invasion and Numbering* (CASPIN); Electronic Privacy Information Center; Information Technology and Innovation Foundation.

[181] *See, e.g.*, RFID Right to Know Act of 2005, S.B. 638, 93rd Gen. Assemb., 2d Reg. Sess. (Mo. 2006) (requiring notice to consumers regarding RFID devices); N.H. Rev. Stat. Ann. § 236:130 (2009) (making it illegal to use RFID tags to determine the ownership of a motor vehicle or to determine the occupants within a motor vehicle).

[182] Demetrius Klitou, *Privacy by Design and Privacy-Invading Technologies: Safeguarding Privacy, Liberty and Security in the 21st Century*, 5 LEGISPRUDENCE 3 (2011).

[183] *Id.*

[184] *See, e.g.*, Wisconsin Statute 146.25; California Civil Code, Section 52.7a;

of RFID technology has not been specifically addressed in legislation. The European Commission (Commission) has issued recommendations RFID applications on the issue but no legislation has yet been passed.[185] This recommendation reiterates that, under the current legislation, the national public authorities are responsible for ensuring the application of national legislation and the protection of personal data.[186] Furthermore, in regards to the security of the RFID system, the Member States, the Commission, and businesses should take concerted action concerning technical and organizational aspects and business procedures. To this end, the Commission encourages the consolidation of good practice and the drawing up of design criteria for RFID technology so risks are restricted from the start. The criticism stands that in order to protect individuals from privacy invading technologies, such as RFID, the international community needs to act in concert and promptly. In so far as the laws are not consistent the risk for privacy violations is ever more evident.

C. Social Networks

As the World Wide Web expanded as a means for individuals to interact, discuss, and share information with one another, social media sites, or networking sites, began to appear. The earliest incarnations of social media on line took the form of chat pages or message boards, where individuals could either chat in real time or leave messages. Social media networks, or pages, have evolved into

---

North Dakota Senate Bill 2415 (2007). It is important to note that these laws do not regulate IRFD but prohibit the involuntary implantation of such devices.

[185] *Commission Recommendation of 12 May 2009 on the Implementation of Privacy and Data Protection Principles in Applications Supported by Radio-Frequency Identification*, 2009 O.J. (L 122) 47-51, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009H0387:EN:HTML.

[186] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*, at 96, COM (2007) 312 final (Mar. 15, 2007), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0096:EN:NOT.

numerous distinct formats ranging from review sites, blogs, wikis, picture and scrap booking, music and file sharing, and social networks. Social networks in particular have had perhaps the greatest growth and the biggest impact on the way people currently interact online. Today, there are some fourteen social media networks with over 100 million registered users.[187]

Social networks can best be defined as web-based services that allow individuals to "(1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."[188] Most social networks share the common characteristic of "visible profiles that display an articulated list of friends who are also users of the system."[189] The very first social network site appeared online in 1997, it was called www.SixDegrees.com and it allowed users to post and send messages to people with whom they were "connected."[190]

As social networks have mushroomed, so has the amount of information and data that individuals are willing and able to post about themselves on these sites. Sites such as Facebook, MySpace, Google+, Instagram, etc, collect data on the interests of their users, their friends, and their preferences for anything from travel information to the games they play. They also collect photographs, location, and many other pieces of information about the users. This

---

[187] *List of Virtual Communities With More Than 100 Million Users*, WIKIPEDIA, http://en.wikipedia.org/wiki/List_of_virtual_communities_with_more_than_100_million_users (last modified Mar. 24, 2013). The article provides that the following statistics: *Facebook* 1+ billion, USA; *Tencent* 712 million, China; *Skype* 663 million, Denmark/Sweden; *Qzone* 536 million, China; *Twitter* 500+ million, USA; *Google+* 400+ million, USA; *Windows Live* 330+ million, USA; *Sina Weibo* 368 million, China; *Tencent Weibo* 310 million, China; *Habbo* 273 million, Finland; *LinkedIn* 175+ million, USA; *Badoo* 162+ million, UK; *VK (VKontakte)* 140+ million, Russia; *Bebo* 117 million, USA. *Id*.

[188] D. M. Boyd & N. B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMMUNICATION, 210–230 (Dec. 2007).

[189] *Id.*

[190] *Id.*

information becomes the source of much concern from a privacy standpoint because once the information is uploaded onto a social network, the site has broad latitude as to how long it can maintain the information, how to use the information, and for what purposes.[191]

Social networks utilize many techniques for information gathering, but the ultimate goal is the generation of revenue for their website. The collection and compilation of users' data creates revenue for an industry that seeks to find sources of revenue based on the ability to provide useful data to advertisers and other industries for both marketing and direct sales. The most effective way to accomplish these aims is by collecting more and more information about the users of the services.[192] In addition to the information that the users themselves disclose when they sign up for the service, such as their address, telephone number, date of birth, etc., the sites also collect information about the device that the user is using to access the site, tracks data about patterns of use of the service, records location information of the user when he or she accesses the site, and may collect other personal information stored in the user's computer using cookies and anonymous identifiers.[193] This ability to capture so much consumer information has not gone unnoticed.

Many groups, governments and other entities have sounded the alarm. For example, The U.S. Food & Drug Administration has held hearings on the "Promotion of FDA-Regulated Medical Products Using the Internet and Social Media Tools;"[194] and the

---

[191] Users grant Facebook, for example, "a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License)…" limited only by Facebook privacy settings. Moreover, this "license" does not end upon deletion or closing on one's account. *Facebook Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/legal/terms (last visited Oct. 17, 2012).

[192] As stated in Google+'s Privacy Statement: "[w]e collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful or the people who matter most to you online." *Policies and Principles*, GOOGLE, http://www.google.com/policies/privacy/ (last visited Oct. 17, 2012).

[193] *Id.*

[194] *See Public Hearing on Promotion of FDA-Regulated Medical Products*

European Union has advocated that in the area of social networks, "[p]rivacy is a vital aspect of social network use. The EESC [European Economic and Social Committee][195] has already presented its views on the proposal for a General Data Protection Regulation, stating its unequivocal support for the right to be forgotten and the preservation of privacy by default, i.e. when consent cannot be implied and must always be given expressly or explicitly."[196]

In 2009, Germany passed amendments to the country's Federal Data Protection Act.[197] These amendments covered a broad range of data collection issues including a requirement of notification of data security breaches[198] and changes in data marketing rules.[199] The 2009 amendments also called for increased fines for violations of the law,[200] and expanded the powers of the supervisory authority.[201] Germany has battled with U.S. technology companies Apple, Facebook, and Google. The country has launched investigations into how these companies collect and store personal data.[202] In one instance, German officials asked Google to turn over data from home wireless networks that were collected while the

---

Using the Internet and Social Media Tools, FOOD AND DRUG ADMIN., http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDER/ucm184250.htm (last visited Oct. 17, 2012).

[195] The European Economic and Social Committee (EESC) is a consultative body that gives representatives of Europe's socio-occupational interest groups, and others, a formal platform to express their points of views on EU issues. *See About the Committee*, EUROPEAN ECONOMIC AND SOCIAL COMMITTEE, http://www.eesc.europa.eu/?i=portal.en.about-the-committee (last visited July 20, 2013).

[196] *See* Bernardo Hernández Bataller, *Responsible use of social networks*, EUROPEAN ECONOMIC AND SOCIAL COMMITTEE, http://www.eesc.europa.eu/?i=portal.en.ten-opinions.22340 (last visited Oct. 17, 2012).

[197] Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Jan. 1, 2002, BGBl. I, last amended by Gesetz [G], Sept. 1, 2009, BGBl. I (Ger.).

[198] *Id.* § 42(a), § 33.

[199] *Id.* § 30(a), § 28(a), § 32.

[200] *Id*. § 43.

[201] *Id.* § 23, § 38.

[202] *Google-Street-View Tours Also Used for Scanning WLAN-Networks*, FED. COMMISSIONER FOR DATA PROTECTION & FREEDOM INFO. (Apr. 23, 2010), http://www.bfdi.bund.de/EN/PublicRelations/PressReleases/2010/GoogleWLANScan.html?nn=410214; *See also* Kevin O'Brien, *Despite Privacy Inquiries, Germans Flock to Google, Facebook and Apple*, N.Y. TIMES, July 12, 2010, at B8.

company compiled information for its Street View map.[203] German officials questioned Apple about the duration and the type of personal information the company stores on its iPhone 4.[204]

German data-protection officials launched legal proceedings in August 2010 because of how Facebook handles non-user information.[205] Facebook's social graph architecture allows any site to share information between the site and the Facebook platform, permitting readers of the German news magazine Spiegel Online[206] to see what stories their Facebook "friends" like, for example.[207] Many websites and online magazines often use a "Like" button to connect their visitors to Facebook, permitting users to promote a particular item with a single click.[208] Many users might assume that no information would be passed to Facebook unless they pressed the "Like" button, but they would be wrong. An executive at a privacy software company offers a startling comparison: "[w]hat people don't realize is that every one of these buttons is like one of those dark video cameras. If you see them, they see you."[209] Facebook admits that the company can see "information such as the IP

---

[203] Kevin O'Brien, *Google Balks at Turning Over Data to Regulators*, N.Y. TIMES, May 28, 2010, at B3.

[204] *Id.*

[205] Christopher Lawton & Vanessa Fuhrmans, *Google Rouses Privacy Concerns in Germany--Mapping Service Sparks Debate as Nation Scarred by Authoritarian Past Grapples With Personal Data in Digital Age*, WALL ST. J., Aug. 17, 2010, at B5.

[206] SPIEGEL ONLINE, http://www.spiegel.de/international/ (last visited July 20, 2013).

[207] In 2010, Facebook opened up its powerful platform, allowing any site in the world to connect to Facebook. Emily Bell, *Why Facebook's Open Graph Idea Must Be Taken Seriously*, GUARDIAN (U.K.) (Apr. 26, 2010), http://www.guardian.co.uk/media/pda/2010/apr/26/facebook-f8-emily-bell.

[208] Spiegel Online's English site calls the Facebook button "Recommend," instead of "Like." *See* kla, with wires, *'Like' Button Battle: Facebook Agrees to Voluntary Privacy Code*, SPIEGEL ONLINE (Sept. 8, 2011), http://www.spiegel.de/international/germany/like-button-battle-facebook-agrees-to-voluntary-privacy-code-a-785190.html.

[209] Riva Richmond, *As 'Like' Buttons Spread, So Do Facebook's Tentacles*, N.Y. TIMES (Sept. 27, 2011), http://bits.blogs.nytimes.com/2011/09/27/as-like-buttons-spread-so-do-facebooks-tentacles/.

address" of users who visit a site with a "Like" button.[210] But it says that it simply collects aggregate data: "According to Facebook, it simply counts the number of Internet Protocol (IP) addresses that visit sites with Like buttons . . . ."[211] The Facebook privacy policy, however, suggests that Facebook receives an array of data when a user visits a website that connects to the Facebook Platform through such links as the "Like" button:

> We receive data whenever you visit a game, application, or website that uses Facebook Platform or visit a site with a Facebook feature (such as a social plugin). This may include the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, if you are logged in to Facebook, your User ID.[212]

In August 2011, the data protection minister for the northern German State of Schleswig-Holstein, Thilo Weichert, declared that the "Like" button and other Facebook actions violated both German and European law.[213] The state data protection authority led by Weichert, the Independent Center for Data Protection for Schleswig-Holstein (the ULD), explained: "Whoever visits facebook.com or uses a plug-in must expect that he or she will be tracked by the company for two years. Facebook builds a broad profile for members

---

[210] Melissa Eddy, *German Privacy Watchdog Dislikes Facebook's 'Like,'* USA TODAY (Aug. 19, 2011), http://www.usatoday.com/tech/news/story/2011/08/German-privacy-watchdog-dislikes-Facebooks-Like/50061684/1.

[211] *Id.* (reporting a Facebook spokesperson's statement that "[w]e delete this technical data within 90 days"); *see also* Stuart Tiffen, *Facebook's 'Like' a Hot Button Issue in Germany*, DEUTSCHE WELLE (GER.) (Sept. 9, 2011), http://www.dw.de/dw/article/0,,15375988,00.html.

[212] *Data Use Policy*, FACEBOOK, https://www.facebook.com/full_data_use_policy (last visited Sept. 23, 2011).

[213] Doug Goss, *German Official: Ditch Facebook's 'Like' Buttons*, CNN (Aug. 19, 2011), http://edition.cnn.com/2011/TECH/social.media/08/19/facebook.germany.like/index.html.

and even a personalized profile. Such profiling infringes German and European data protection law."[214] The ULD thus directed websites based in the state to desist from connecting their site to Facebook through the "Like" button subject to a penalty of up to 50,000 euros. The ULD also directed government agencies to shutter their own Facebook pages.[215] The Schleswig-Holstein Tourism Agency was one of the entities that complied with the ruling, pulling its Facebook page. While noting that the Tourism Agency takes issues of privacy very seriously, a spokeswoman for the agency also "bemoaned the loss of the tools provided by the social media platform, saying they had been useful for business."[216]

In response to these complaints, Facebook announced in September of 2011 that it would abide by a voluntary code of conduct in Germany to protect user data. According to reports, this was "the first time the site has agreed to such measures."[217] The details of this code of conduct have not been published to date. Facebook has not smoothed its relations with all German authorities, however. In November 2011, the data protection authority of the German State of Hamburg said that it planned to initiate legal action against Facebook for a new feature that automatically recognizes faces in photos posted to the site.[218] The Hamburg authority complained that Facebook had introduced this feature without seeking user consent. Indeed, in the U.S., at least, the feature is activated by default, though an individual can disable it if he or she

---

[214] Press Release, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein [the Independent Center for Data Protection for Schleswig-Holstein (ULD)], ULD to Website Owners: "Deactivate Facebook Web Analytics," (Aug. 19, 2011), https:// www.datenschutzzentrum.de/presse/20110819-facebook-en.htm.

[215] *Id.*

[216] Tiffen, *supra* note 211.

[217] *German Minister Advises Colleagues to Shun Facebook*, AGENCE FRANCE-PRESSE (FR.) (Sept. 11, 2011), http://www.google.com/hostednews/afp/article/ALeqM5hyxHKd75Jl0hl_RfeclhEvMPZ8w?docId=CNG.ee29706d29744c955731a90381f66cc5.831.

[218] Cyrus Farivar, *Hamburg Considers Suing Facebook Over Facial Recognition Feature*, DEUTSCHE WELLE (GER.) (Nov. 10, 2011), http://www.dw-world.de/dw/article/0,15523030,00.html.

chooses.[219]

France has also battled Facebook. In *Hervé G. v. Facebook France*, the Paris Court of First Instance considered a claim brought by French Bishop Hervé Giraud of Soissons against Facebook.[220] Bishop Hervé Giraud of Soissons claimed that a Facebook page titled "*Courir nu dans une église en poursuivant l'évêque*" (running naked in a church after the bishop) incited hate and violence against Catholics and, thus, violated the French hate speech codes.[221] He also claimed that his photograph was used without his permission.[222] The French court ruled in the bishop's favor on both grounds.[223] Even though the photograph at issue was not at all scandalous, but rather simply a portrait of the bishop,[224] the French court ordered Facebook to remove the page, and to pay 2,000 Euros in damages, with a penalty for every day the page remained up.[225]

Generally, privacy becomes a concern as a reaction to events and advancements that facilitate its infringement. Thus, the legal protection of private personal data has become more of a necessity for individuals as technology has made the collection, distribution, and transfer of information faster and more efficient. As technology advances it becomes easier to access individuals' personal information without much effort or training, merely by pressing a button on a computer terminal. The impact of digital technology on privacy appears to follow the same pattern seen with older technologies, and one can foresee that the law will attempt to evolve

---

[219] *See* Matt Elliott, *How To Disable Facial Recognition in Facebook*, CNET (June 8, 2011), http://howto.cnet.com/8301-11310_39-20070045-285/how-to-disable-facial-recognition-in-facebook/.

[220] Hervé G. v. Facebook France (TGI Paris, April 13, 2010).

[221] *Id.*

[222] *Id.*

[223] *Id.*

[224] *See* Joséphine Bataille, *Condamné pour Outrage à un Évêque, Facebook Gagne en Appel*, LA VIE (FR.) (Nov. 1, 2011), http://www.lavie.fr/actualite/france/condamne-pour-outrage-a-un-eveque-facebook-gagne-en-appel-11-01-2011-13046_4.php (providing an image of the Facebook page).

[225] *Id.*

in response to the privacy threats posed by the digital revolution.[226] But the impact of the digital age is so deep and pervasive that expansion of a single area of privacy law is unlikely to adequately address all of the problems.[227] Since the digital age affects every aspect of privacy, it requires an evolution, not just in the existing framework, but also in the very conceptual and legal status of privacy. The response to the effect of new technologies on our concept of privacy has usually been greater governmental regulation.[228] However, greater regulation might not adequately address privacy violations on the part of governments and private

---

[226] *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1374 (2000).

[227] *See* William S. Challis & Ann Cavoukian, *The Case of a U.S. Privacy Commissioner: a Canadian Commissioner's Perspective*, 19 J. MARSHALL J. COMPUTER & INFO. L. 1 (2000) (arguing that the current regulatory system with regards to new technologies and their effect on privacy is insufficient). The author makes the case for the creation of a specialized agency headed by a U.S. Privacy Commissioner with the responsibility of establishing fair information practices and standards in the context of businesses and technologies. *Id.*

[228] See Directive 95/46/EC, of the European Parliament and the Council of 24 October 1995, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281), *available at* http://europa.eu/legislation_summaries/information_society/l14012_en.htm, for examples of state regulation initiatives; Freedom of Information Act, 5 U.S.C. § 552 (2000), *available at* http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm; Right to Financial Privacy Act, 12 U.S.C. § 3412 (2000), *available at* http://www.law.cornell.edu/uscode/text/12/3412; Privacy Protection Act, 42 U.S.C. § 2000 (2000), *available at* http://www.law.cornell.edu/uscode/42/2000aa.html; Employee Polygraph Protection Act, 29 U.S.C.S. §§ 2001 et seq. (2000), *available at* http://www.law.cornell.edu/uscode/29/usc_sup_01_29_10_22.html; Cable Communications Policy Act, 47 U.S.C. §551(h) (2000), *available at* http://www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000551----000-.html; Financial Services Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999), *available at* http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/content-detail.html; The Children's Online Privacy Protection, 15 U.S.C. §§ 6501-6506 (1999), *available at* http://www.law.cornell.edu/uscode/html/uscode15/usc_sup_01_15_10_91.html; Personal Information Protection and Electronic Documents Act, S.C. ch. V (2000) (Can.) (assented to Apr. 13, 2000), *available at* http://www.priv.gc.ca/information/guide_e.pdf; The Australian Privacy Commission, Australia's Privacy Amendment (Bill 2000), *available at* http://www.privacy.gov.au/law/act (last viewed Oct. 17, 2012).

parties that utilize the latest technologies. A combination of state regulation, as well as legal protections for the individual, must be devised in order to keep up with the technology that makes possible unfettered invasions of privacy.

III. Recommendations for the Protection of Privacy in Today's World: Consumer Awareness, Value Sensitive Design and Effective Legal Action

Technology is generally constructive for society as most of the innovations from technological advances have very important positive effects on the lives of people throughout the world. However, technology can be both a threat and a solution to protecting privacy; it can provide the powerful instruments of surveillance and privacy intrusion, but also the effective controls over privacy-invading technology. It is impossible to fully predict the effects of new technologies on privacy or to impede their development.[229] To think that the current legislative process will

---

[229] For instance, a new technology referred to as The SixthSense Technology, being developed by Pranav Mistry and the MIT Media Lab, allows an individual to have immediate access to all of the information on the Internet about a person only by looking at them (and wearing the sixth sense technology device). *See* Pranav Mistry, *About*, SIXTHSENSE, http://www.pranavmistry.com/projects/sixthsense/ (last visited Jan. 18, 2013).

The SixthSense prototype is comprised of a pocket projector, a mirror and a camera. The hardware components are coupled in a pendant like mobile wearable device. Both the projector and the camera are connected to the mobile computing device in the user's pocket. The projector projects visual information enabling surfaces, walls and physical objects around us to be used as interfaces; while the camera recognizes and tracks user's hand gestures and physical objects using computer-vision based techniques. The software program processes the video stream data captured by the camera and tracks the locations of the colored markers (visual tracking fiducials) at the tip of the user's fingers using simple computer-vision techniques. The movements and arrangements of these fiducials are interpreted into gestures that act as interaction instructions for the projected application interfaces. *Id.*

According to the creators: "SixthSense bridges the gap between the digital and the physical world, bringing intangible, digital information out into the tangible world, and allowing us to interact with this information via natural hand

prevent abuses on privacy by new technologies is unrealistic, as privacy-invading technologies evolve faster than privacy protecting laws. Thus, controlling the effects of technology should not be left exclusively in the hands of legislators or judges, whose rulings are often rushed to meet the urgency of the case at hand. It has been suggested that technology should be regulated at the design and manufacture stage through what is generally referred to as Value Sensitive Design (VSD).[230]

VSD is a theoretically grounded approach based on aiming to control or regulate the intrusive capabilities of the technologies concerned, embedding ethics and human values in a principled and comprehensive manner in the design and manufacture of technology.[231] VSD maintains certain values that are universally held, such as those that pertain to human welfare, rights, and justice, in the design and manufacture of technology.[232] Additionally, VSD adopts the position that technologies in general, information and computer technologies in particular, provide value suitabilities that follow from properties of the technology.[233] In order to achieve the appropriate engineering scheme, different techniques are used. Among them is what some refer to as "technical investigations," which focus on "how existing technological properties and

---

gestures. 'SixthSense' frees information from its confines by seamlessly integrating it with reality, and thus making the entire world your computer." *See Id; see also* Clark Boyd, *SixthSense blurs digital and the real,* BBC TECHNOLOGY (April 14, 2009), *http://news.bbc.co.uk/2/hi/technology/7997961.stm*.

[230] *See, e.g.*, K. A. Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 7 YALE J. L. & TECH. 123, 126-127 (2004-05) (writing that: "[i]n a technologically mediated information society, civil liberties can only be protected by employing value sensitive technology development strategies in conjunction with policy implementations, not by opposing technological developments or seeking to control the use of particular technologies or techniques after the fact through law alone").

[231] *See* Sorning et al., *supra* note 10, at 68-69 (discussing development of value added design and its applicability to respecting human values).

[232] Taipale, s*upra* note 230, at 127.

[233] J. C. Thomas, *Steps Toward Universal Access Within a Communications Company*, *in* HUMAN VALUES AND THE DESIGN OF COMPUTER TECHNOLOGY 271-287 (B. Friedman ed., 1997).

underlying mechanisms support or hinder human values."[234] For example, one might design a video recording system that provides blurred views of an office setting allowing for some modicum of privacy, while other systems may instead provide clear images that reveal detailed information about who is present and what they are doing. The two designs differentially adjudicate the value trade-off between an individual's privacy and the individual's presence in the office.

VSD places a great part of the responsibility on designers and manufacturers on predicting the future effect of technology at the time the technology is being created. The designers and manufacturers of new technologies are better equipped to forecast how new technologies can be misused. Therefore, VSD recognizes the designers and manufacturer's role in devising ways to help prevent technologies' negative effects on society. As to privacy invading technologies, "privacy by design" promotes designing information and communications technologies (ICT) and building privacy into the product or technology from the outset.[235] Privacy by design is not a specific technology or product, but a systematic approach to designing any technology that embeds privacy into the underlying specifications or architecture. Privacy by design has two main elements when it comes to technology: first, incorporating substantive privacy protections into a firm's practices; and second, maintaining comprehensive data management procedures throughout the life cycle of their products and services.[236]

Information and consumer awareness, regarding the effect of technologies on their privacy, is critical to avoid the detrimental effects of privacy invading technologies. Most users of technologies are not aware of how to manipulate the special program settings that provide protection.[237] Privacy-Enhancing Technologies (PETs) are

---

[234] Sorning et al., *supra* note 10, at 69.

[235] *See* Cavoukian, *supra* note 11.

[236] Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change*, FEDERAL TRADE COMMISSION (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[237] Ira Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 274-77 (2008)

applications or tools with discrete goals that address a single dimension of privacy, such as anonymity, confidentiality, or control over personal information. Frequently, PETs are added onto existing systems, sometimes as an afterthought by designers and sometimes by privacy-sensitive end-users.[238] Given that it is ever more difficult for consumers to learn about the different functions of a certain program, application, or internet site that might infringe on the user's privacy,[239] it is reasonable to expect manufacturers to provide information to consumers regarding their technology and its effect on their privacy, as well as to establish settings that are privacy protecting from the outset. Informed consent provides a critical protection for privacy, and supports other human values such as autonomy and trust. Privacy by Default[240] or Opt-In Standard[241] as a

(discussing underutilization of anonymity tools due to apathy, consumer ignorance, and difficulty in finding, understanding, and configuring the relevant tools).

[238] Many PETs now take the form of so-called "browser add-ons." *See* Brock, *supra* note 12.

[239] One example is the use of cookies to monitor behavior of users of the Internet. Cookies are small text files placed on a user's computer to store information about the user's preferences. Websites use cookies both to offer a personalized experience to users and to track online behavior and usage patterns in order to tailor online ads to groups of users based on demographics or likely purchasing behavior. Cookies are often placed without users' express knowledge or consent; they raise privacy concerns because they capture and transmit data about individual users. This information can include the searches that users have run, the identifying information that they have disclosed, their browsing patterns while visiting a site, and their "clickstream" behavior, which is the link the user clicked while browsing the web. *See In re* DoubleClick Inc Privacy Litigation, 154 F. Supp. 2d 497, 504-05 (SDNY 2001) (describing how DoubleClick employs cookies to record a user's browsing history while visiting DoubleClick-affiliated websites).

[240] 'Privacy by design' and 'privacy by default' mean that, "privacy safeguards will have to be integrated into products as they are developed and that in social networking, the default settings must protect the privacy of individuals." Neil Hodge, *The EU: Privacy by Default*, 8 IN-HOUSE PERSPECTIVE 19 (Apr. 2, 2012).

[241] "Opt-in permits use of personal information within the organization but requires the opt-in consent before personal information could be disclosed to third parties outside the organization." Jan Bouckaert & Hans Degryse, *Opt In Versus Opt Out: A Free-Entry Analysis of Privacy Policies*, CENTER - TILBURG UNIVERSITY 3, *available at* http://weis2006.econinfosec.org/docs/34.pdf (last

privacy enhancing technology should be compulsory, and the responsibility of designers and manufacturers.

The law needs to be proactive regarding privacy issues. The future of privacy depends on creating preventive laws and regulations in a holistic manner, rather than responding to individual crisis affecting privacy. In order to achieve better results, jurists and legislators must partner with designers and manufacturers of technology, as well as privacy and other experts, to create laws that address potential issues regarding privacy. Privacy officials in Europe and the U.S. are embracing privacy by design by addressing privacy concerns of new technologies.[242] Proposals have been made that would create a framework in the development of privacy by design technologies, such as the creation of new regulatory agencies able to receive input from experts from industry, advocacy groups,

---

visited 19 June 2013).

[242] The European Union Data Protection Directive has always included provisions requiring data controllers to implement "technical and organizational measures" in the design and operation of ICT. *See* Directive 95/46/EC, 1995 O.J. (L 281) 31 (Nov. 23, 1995), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML. Council Directive 95/46 requires data controllers to "implement appropriate technical and organizational measures" for safeguarding personal data. *Id.* In addition, Recital 46 calls for such measures to be taken, "both at the time of the design of the processing system and at the time of the processing itself." *Id.* The European Commission (EC) hopes to see data protection principles taken into account at the outset of designing, producing, or acquiring ICT systems. They are encouraging both the use of Privacy Enhancing Technologies, or PETs, as well as default settings that favor privacy. *See* Art. 29 Data Protection Working Party & Working Party on Police and Justice, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* (Dec. 1, 2009), *available at* ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/ wp168_en.pdf; John J. Borking & Charles D. Raab, *Laws, PETs and Other Technologies for Privacy Protection*, 2001 J. INFO L. & TECH., no. 1, *available at* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking/. In the United States, a recent staff report of the Federal Trade Commission (FTC) describes a Proposed Framework with three main components: privacy by design, simplified consumer choice, and increased transparency of data practices. According to the Staff Report, companies engage in privacy by design when they promote consumer privacy throughout their organizations and at every stage of the development of their products and services. *See* Preliminary FTC Staff Report, *supra* note 236.

and academia to oversee privacy by design and overcome the prejudicial dichotomy of purely voluntary industry codes of conduct versus highly prescriptive government regulation.[243] Such schemes would also help encourage innovation and experimentation with privacy technology.[244]

Conclusion

It is clear that in combination, globalization and technology have changed the world and affected society in immeasurable ways. Technology not only brings about innovation and progress for civilization, but also brings the potential to harm society and the principles we cherish as individuals. Today, data protection appears to be at the forefront of privacy concerns because people are worried about their privacy. In response to the overwhelming demand for privacy, governments are enacting laws that protect people's privacy in this digital era. Technology, with its potential to infringe on privacy rights, also has the potential to provide protection from privacy violations. While computer programs are created to collect and distribute user's digital information, programs are also created to help users keep their personal digital information private.[245]

Society must find the way to adapt to new developments in order to preserve its values and its humanity. As such, the future of privacy depends on politicians, legislators, educators, students, designers of technology, judges, and journalists, among many others. Everyone has a stake in privacy, and everyone has an obligation to protect one of the most important values of human beings. It is

---

[243] Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409 (Symposium 2011).

[244] Rubinstein, *supra* note 243.

[245] *See, e.g.*, PrivacyFix, which is a program that helps set up a user's privacy settings on Facebook and Google, and control cookie activity. *Welcome to your (free) privacy dashboard*, PRIVACYFIX, https://www.privacyfix.com/start (last viewed Jan. 18, 2013); *see also* Lance Whitney, *PrivacyFix helps protect your privacy on the Web*, CNET.COM (Oct. 10, 2012), http://news.cnet.com/8301-1009_3-57529655-83/privacyfix-helps-protect-your-privacy-on-the-web/ (reviewing and explaining the benefits of PrivacyFix).

difficult to predict, or even to imagine, the technology that the future will bring, but positive strides are being made in the recognition that the protection of privacy is as much of an obligation of the consumers of technology as to the designers and manufacturers of technology. We must continue on the line of sharing in the obligations for the protection of privacy on more than just the distributors and end users of technology. Privacy is everyone's concern and everyone should be involved in protecting the human value it represents.