PRIVACY AND SECURITY POST-SNOWDEN: SURVEILLANCE LAW AND POLICY IN THE UNITED STATES AND INDIA

ZACHARY W. SMITH*

Introduction

The June 2013 interview between Guardian journalist Glenn Greenwald and now famed National Security Agency (NSA)[1] whistleblower Edward Snowden[2] (Snowden) introduced the world to the NSA's data mining[3] operation, known as "PRISM."[4] Snowden

* Zachary W. Smith, J.D.'14, *cum laude*, St. Thomas University School of Law; B.A. cum laude in History, Phi Beta Kappa, University of Florida. I want to give a special thank you to Gabriela Schoepflin for her outstanding assistance in editing this article. I also owe a debt of gratitude to Professor Siegfried Wiessner for his invaluable guidance and mentorship during my time at St. Thomas University.

[1] *See* S. SELECT COMM. ON GOV'T OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FOREIGN AND MILITARY INTELLIGENCE, 94TH CONG. (Comm. Print 1976). The National Security Agency is an arm of the American intelligence community that monitors foreign electrical communications for the purpose of identifying potential security threats to classified American interests. Sensitive information acquired during its collection process is used to aid other intelligence agencies, including the Central Intelligence Agency (CIA), in their top-secret operations domestically and internationally.

[2] Jaikumar Vijayan, *Snowden's Role Provided Perfect Cover for NSA Data Theft*, COMPUTERWORLD (Sep. 19, 2013), *available at* http://www.computerworld.com/article/9242493/Snowden_s_role_provided_perfect_cover_for_NSA_data_theft. Edward Snowden was employed by the NSA as a systems administrator with top-secret clearance. *Id.* With top-secret clearance, Snowden had easy access to NSA documents, including "power-point slides, secret court orders, and classified agency reports." *Id.* Snowden's dissemination of confidential NSA documents changed the agency's prior position on employee access to privileged information. *Id.* System administrators, in particular, are no longer permitted to conduct their work in secret. *Id.*

[3] *See* T.Y. Lin et al. *Security and Data Mining, in* DATABASE SECURITY IX STATUS AND PROSPECTS 391, 394 (D.L Spooner et.al, ed. 1996), available *at* http://xanadu.cs.sjsu.edu/~drtylin/publications/paperList/76_08dnfina3.pdf. Data mining is a specialized practice involving the acquisition of large quantities of information to identify patterns in behavior. *Id.* These patterns are then gathered to draw various inferences about a particular behavioral trait. *Id.*

showcased audacious undertakings occurring overseas, including spy games during diplomatic conferences with world leaders,[5] and the storage of personal data at a one-million square foot site in the Utah Desert.[6] By proffering these allegations to the world at a time when social media[7] has developed into a popular mode of communication,[8]

---

[4] Didier Bigo et al., *Open Season for Data Fishing on the Web*: *The Challenges of the US PRISM Programme*, 293 CTR. FOR EUR. STUDIES (June 18, 2013), *available at* http://aei.pitt.edu/42429/1/PB293_Bigo_et_al_Prism_ Programme_ (1).pdf. NSA employs PRISM, a controversial surveillance program that facilitates access to the private information of citizens and governmental institutions. *Id.* Past uses of PRISM have involved, for example, the warrantless interception of data running through fiber optic cables of a prominent telecommunications company. *Id.*

[5] *See* Ewen MacAskill et al., *GCHQ Intercepted Foreign Politicians' Communications at G20 Summits*, THE GUARDIAN (Jun. 16, 2013), http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits. During the G20 summit in April and September 2009, British intelligence demonstrated its proficiency in data collection when its agents used sophisticated monitoring devices to eavesdrop on participating delegations, in particular Turkey and Russia, to establish the relative positions of countries following the global economic meltdown in 2008. *Id. See G-20 Members, available at* https://www.g20.org/about_g-20/g20_members (last viewed Feb. 11, 2014). The G-20 summit is meeting of finance ministers and central bank governors from 19 countries (Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, The Republic of Korea, Mexico, Russia, Saudi Arabia, South Africa, Turkey, the United Kingdom, the United States of America, and the European Union). *Id. See also G-20 Priorities, available at* https://www.g20.org/g20_priorities (last viewed Feb. 11, 2014). The aim of the G-20 is to formulate financial regulations that further economic growth and prevent future economic crises. *Id. See* Cindy Cohn, *Lawless Surveillance and Warrantless Rationales*, 8 J. TELECOMM. & HIGH TECH L. 351, 354 (2010) (citing STEVE WRIGHT, EUROPEAN PARLIAMENT, DIRECTORATE GENERAL FOR RESEARCH, AN APPRAISAL OF TECHNOLOGIES OF POLITICAL CONTROL (1998)). A European Parliament study confirmed the existence of comprehensive listening posts operated by the NSA, designed to retrieve significant amounts of foreign communications. *Id.*

[6] *See* Cohn, *supra* note 5, at 353. The construction of the Utah facility and a secondary facility in Texas "will be used to store trillions of phone calls, e-mail messages, and data trails: web searches, parking receipts, bookstore visits, and other digital 'pocket litter'." *Id.*

[7] *See* Andreas M. Kaplan & Michael Haenlein, *Users of the World, Unite! The Challenges and Opportunities of Social Media*, 53 BUS. HORIZONS 59, 61 (2010). Social media is a creative process by which individuals engage interactively

and at a time when the amount of information traversing over the internet has never been higher,[9] Snowden has refocused our attention on the state of informational privacy[10] and the need for more transparency on privacy rules in the international arena.[11] The opinion of this author is that despite the creation of privacy laws, the privacy laws that exist today across a large swath of the industrialized world are inherently inadequate to address the intrusive nature of communications technology, which has grown excessively under the vanguard of interconnectedness and openness. The paper is organized in a dual format, through the lens of two behemoths within the information technology sector: the United States[12] and India.[13] While India is an emerging superpower just

---

through the publishing of media content on the internet in order to exchange ideas and influence behavior. *Id.*

[8] ERIK QUALMAN, SOCIALNOMICS: HOW SOCIAL MEDIA TRANSFORMS THE WAY WE LIVE AND DO BUSINESS, foreword (2nd ed. 2013). Social media has had a profound impact on the management structure of the British Broadcasting Company (BBC), the budget of Ford Company's Marketing Division, the attention given to revolutionary uprisings as the one seen in Iran, and the philanthropic mission in Haiti following their devastating earthquake. *Id.*

[9] RONALD J. DEIBERT, BLACK CODE: INSIDE THE BATTLE FOR CYBERSPACE 52 (2013). To illustrate the sheer volume of data exchanged globally, the author gives the following statistics:

> In 2011, 200 million tweets were posted everyday (and over 30 billion have been written and sent since Twitter's launch in 2006). Every sixty seconds, 168 emails were sent, nearly 700,000 Google searches and Facebook status updates made, 375,000 Skype calls initiated, and 13,000 IPhone apps downloaded.

Id.

[10] *See* A. Michael Froomkin, *The Death of Privacy?* 52 STAN. L. REV. 1461, 1464 (May, 2000). Froomkin defines informational privacy as the "ability to control the acquisition or release of information about oneself." *Id.*

[11] *See* Gene Healy, *Spying's the Story, Not Edward Snowden*, CATO INST. (Jun. 24, 2013). Unfettered access into the private phone calls and records of individual citizens could create a perfect storm in terms of political abuse and blackmail while jeopardizing freedoms and privacy rights. *Id.*

[12] U.S. DEP'T. OF COMMERCE, THE SOFTWARE AND INFORMATION TECHNOLOGY SERVICES INDUSTRY IN THE UNITED STATES, *available at* http://selectusa.commerce.gov/industry-snapshots/software-and-information-technology-services-industry-united-states (last visited Feb. 23, 2014). The important statistic to note in this snapshot of the U.S. information technology (IT)

beginning to recognize the role of information privacy in its society,[14] the United States has a long paper trail of attempts to establish a settled framework for privacy enforcement.[15] This article is subdivided into five sections in accordance with the New Haven[16]

---

sector is the growth and demand in the United States for cloud computing services. *Id.* By 2015, "public cloud computing services will grow four times as fast as information technology spending generally, increasing by 27.6 percent year-on-year from $21 billion in 2010 to more than $76 billion in 2015." *Id.* Out of this projected $76 billion demand in cloud computing services, the United States is projected to constitute 50% of this demand. *Id.*

[13] Sunil Mani, *The Mobile Communications Services Industry in India: Has It Led to India Becoming a Manufacturing Hub for Telecommunications Equipment?* 13 (Ctr. For Dev. Studies, Working Paper no. 444, Apr. 2011). The boom in the Indian telecommunications sector occurred in part due to the Indian government "[increasing] the size of the telecommunications market by first promoting competition between service providers and then by regulating their market conducts through an independent regulatory agency." *Id.* Consequently, "increased competition coupled with regulation reduced telecommunications tariffs which resulted in India having the cheapest telecom services in the world*." Id.*

[14] Dr. Shobhalata V. Udapudi & Barnik Ghosh, *The Information Technology Act of India: A Critique*, 2 ZENITH INT'L J. OF BUS. ECON. & MGMT. RESEARCH 182, 182 (May, 2012). The Information Technology Act (IT Act) was enacted to address a number of security issues associated with the rise in technological transactions at the turn of the century. *Id.* The IT Act also pioneered the move toward the creation of cyber law standards in India. *Id.*

[15] Derek S. Witte, *Bleeding Data in a Pool of Sharks: The Anathema of Privacy in a World of Digital Sharing and Electronic Discovery*, 64 S.C. L. REV 717, 742 (2013). Federal statutes have enumerated protections designed to safeguard personal data from third party observers. However, their role in deterring unauthorized collection of private information is weakened by the individual's choice to disseminate his information as he pleases. *Id.*

[16] W. Michael Reisman, Siegfried Wiessner & Andrew R. Willard, *The New Haven School: A Brief Introduction*, 32 YALE J. INT'L L. 575, 576 (2007).

> The New Haven School defines law as a process of decision that is both authoritative and controlling; it places past such decisions in the illuminating light of their conditioning factors, both environmental and predispositional, and appraises decision trends for their compatibility with clarified goals; it forecasts, to the extent possible, alternative future decisions and their consequences; and it provides conceptual tools for those using it to invent and appraise alternative decisions, constitutive arrangements, and courses of action using the guiding light of the preferred future world public order of human dignity …[A] public order of human dignity is defined as one which approximates the optimum

approach to give the reader comprehensive insight into the vexing issues that surround the information privacy debate today. Part I provides an interdisciplinary perspective into the rise of the surveillance state and questions whether governments can rein in highly-sophisticated technology to ensure equilibrium between individual privacy and national security. Part II outlines a general privacy claim in the current era of mass surveillance, taking into account the perspectives of privacy advocates and the intelligence community as a vehicle to identify the various values at play. Part III documents past trends in decision-making that have shaped the current information privacy infrastructure in the United States and India taking into account the growth of the surveillance state. Part IV sheds light on the future privacy landscape and the growth of the surveillance state following the NSA scandal. In Part V, this author will recommend a privacy framework that can exist transnationally and effectively balance national security interests and personal privacy rights.

I. Delimitation of the Problem

The growth of the information technology sphere has garnered great attention among researchers seeking to deconstruct, both qualitatively and quantitatively, the effect of government misuse of personal data and the consequences for individual privacy.[17] Political scientists have documented this concern in a recent joint empirical study conducted between Hacettepe University (Turkey), the University of Massachusetts (United States), and Huazhong Agricultural University (China).[18] University students were asked to explain their perspectives on electronic surveillance

> access by all human beings to all things they cherish: power, wealth, enlightenment, skill, well-being, affection, respect, and rectitude.

Id. at 576.

[17] *See* Dr. Mehmet Devrim Aydin et.al. *Perception of Surveillance: An Empirical Study in Turkey, USA, and China*, 3 INT'L J. BUS. HUM. & TECH 69, 69 (Apr. 2013), *available at* http://www.ijbhtnet.com/journals/Vol_3_No_4_April_2013/7.pdf.

[18] *Id*. at 71.

and "their perception of threats to privacy arising from IT practices."[19] A total of 249 students answered the questionnaire across the three schools with responses measured on a scale of 1 (strongly disagree) and 5 (strongly agree) with a 3.5 or higher creating the presumption that a threat existed.[20] On the perception of threats to privacy stemming from electronic surveillance, students were asked to respond, according to the scale, to the following questions:

> (1) Surveillance of e-mails and telephones in the workplace by employers
> (2) Surveillance by government over websites
> (3) Surveillance by university over campus members' internet activities
> (4) Security cameras in the dormitories
> (5) Surveillance of citizen's emails and telephones by government officials
> (6) Security cameras in the campus
> (7) Security cameras in the workplace
> (8) Security cameras in the street.[21]

The average for all three schools fell below 3.5, which indicated a relatively low concern for electronic surveillance among the three countries.[22] In their concluding remarks, the authors of the

---

[19] *Id.* To avoid confusion, the study used "IT practices" and "electronic surveillance" interchangeably.

[20] *Id.* at 72.

[21] *Id*.

[22] *Id.* However, for an explanation as to the reasoning behind this attitude, *see* Claire Gordon, *Survey 1 in 6 Writers have Self-Censored Because of NSA Surveillance*, AL-JAZEERA AMER. (Nov. 21, 2013), *available at* http://america.aljazeera.com/watch/shows/america-tonight/america-tonight-blog/2013/11/21/survey-1-in-6-writershaveselfcensoredbecauseofnsasurveillance.html. A July 2013 Pew Center Research Poll noted half of Americans approve of the NSA's bulk collection of phone records. *Id.* However, this reaction may be as a result of the framing of the question; "most of the time the question is phrased as one of security versus privacy and a majority of Americans favor the former." *Id.* Some think the question should be framed more toward how the "government adapts to new technologies, which some believe are perfectly justified, and its

study highlighted that surveillance of communications-based channels, including internet and email were seen as potential infringements on liberties; whereas security cameras positioned in public places did not achieve the same reaction.[23]

Researchers have studied the mixed reaction to responses over privacy and surveillance. A psychological study conducted by Finnish researchers exposed individuals to a closed environment completely subsumed in surveillance technology. Ten households, composed collectively of 12 participants, were wired with "video cameras, microphones, and logging software for personal computers, wireless networks, smartphones, TVs, and DVDs."[24] Stress levels were documented at six and twelve month intervals.[25] At the outset, 11 of the 12 participants stated the "surveillance system proved to be the cause of annoyance, concern, anxiety, and even anger."[26] At the six month interval, some participants decided to exit the study due to the lack of seclusion and the intolerable nature of continuous overexposure.[27] Despite the departure of some participants, the concerns of the remaining subjects subsided as they grew more accustomed to the presence of the surveillance apparatus and adjusted their lifestyle accordingly.[28] However, the behavioral researchers noted a computer logging mechanism installed during the experiment was deemed as obtrusive as the cameras situated around the premises.[29] The researchers commented that this reaction was a response to the idea that computers foster the "anonymity of conversations," and such a logging device that documents the source of the communication created the opposite effect.[30] Specialists in the

---

impact on individual freedoms." *Id.*

[23] Aydin, *supra* note 17, at 76.

[24] Aalto University (Finland), *Negative Effects of Computerized Surveillance at Home: Cause of Annoyance, Concern, Anxiety and Even Anger*, SCIENCE DAILY (Oct. 8, 2012), *available at* http://www.sciencedaily.com/releases/2012/10/121008101646.htm.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

field of management have chronicled the increased use of surveillance technology by business owners toward their employees as a way to improve the overall operational efficiency of the workplace.[31] The American Management Association (AMA) noted in 2001 that "82% of employers are using some form of electronic monitoring the workplace."[32] In 2003, "52% of organizations monitored and tracked email communications alone" and "as high as 92% of all organizations electronically monitor or track their employees in one form or another."[33]

Geographers have argued the continued use of electronic exchanges, such as the internet, to transmit information has given way to a virtual reality, where traditional physical boundaries are replaced by unconventional forums that allow unprecedented access to information in the remotest of locations.[34] Studies recalling the growth of social activism in the 1960s-1970s have referenced the role surveillance played in affecting the organizational dynamic of dissident movements.[35] Since the success of these movements was contingent on their ability to expand their sphere of influence across a wide area and empower individuals to align with their cause, the threat of surveillance heightened fears among members that their communications would become a tool used by authorities to

---

[31] Sherri Coultrup & Patrick D. Fountain, *Effects of Electronic Monitoring and Surveillance on the Psychological Contract of Employees: An Exploratory Study*, AMER. SOC. BUS & BEHAV. SCI. 219 (Feb. 2012), *available at* http://asbbs.org/files/ASBBS2012V1/PDF/C/CoultrupS.pdf. Employers bolster their monitoring capabilities through "electronic monitoring of email communications, website viewing, computer keystroke capturing, listening in on phone calls, video surveillance, etc." *Id.* This monitoring ability has aimed to "increase performance, decreases abuses and/or waste, and control undesirable employee behaviors." *Id.*

[32] *Id.*

[33] *Id.* at 219-20.

[34] Robert M. Kitchin, *Toward Geographies of Cyberspace*, 22 PROGRESS IN HUM. GEO. 385, 386 (1998).

[35] Jules Boykoff, Professor of Politics and Government, Pacific University, *Surveillance, Spatial Compression, and Scale: The FBI and Martin Luther King Jr.* 732 (2007), *available at* http://julesboykoff.org/wp-content/uploads/2013/06/Boykoff-Antipode-article-1.pdf.

prosecute them in a court of law.[36] By intimidating social movements from espousing their beliefs, dissident citizens grew more paranoid in revealing their agenda to the public and in some cases even questioned whether or not to dissent at all.[37] A related study conducted by the PEN American Center, a group that aims at securing freedom of expression and human rights interviewed "more than 500 writers . . . [with] one in six say[ing] they had avoided writing or speaking about a certain topic; and one in four report[ing] they had self-censored via email or on the phone."[38] The same study also stated, "16% of survey respondents refrained from conducting internet searches or visiting websites on topics that may be considered controversial or suspect."[39] In communicating with sources abroad, "39% of the respondents thought it was 'very likely' that a phone call made to a region of the world known to be hostile to the United States would be recorded."[40]

Developments in surveillance have also given rise to emerging disciplines, including Privacy Preserving Data Mining (PPDM).[41] PPDM focuses on deconstructing data mining algorithms to locate cases of potential privacy infringement.[42] PPDM

---

[36] *Id.*

[37] *Id.* at 745; *see also Dissident and Opposition Groups Afraid of NSA Surveillance Sharing*, ACCURACY IN MEDIA (Jun. 15, 2013), *available at* http://www.aim.org/newswire/dissident-and-opposition-groups-afraid-of-nsa-surveillance-sharing/. The article provides the example of a Malaysian Opposition Group, the Democratic Action Party, who cited fears that the growth of monitoring phone calls and emails in the United States will leave their communications vulnerable to interception by their authoritarian government. *Id.* Members of the Democratic Action Party stated they "share a lot of sensitive data, election-related data, using Google Docs." *Id.*

[38] Gordon, *supra* note 22.

[39] *Id.* Participants in the survey expressed qualms commenting on issues of "national security, the Middle East, drug wars, liberal organizing like the Occupy Movement, and child abuse and child pornography*." Id.*

[40] *Id.*

[41] *See* Xiaodan Wu et al. *Privacy Preserving Data Mining Research: Current Status and Key Issues*, *in* COMPUTATIONAL SCIENCE-ICCS 2007 PART III 762, 762 (Y. Shi et.al. eds. 2007), *available at* http://link.springer.com/book/10.1007/978-3-540-72588-6.

[42] *Id.* at 762. PPDM adheres to a number of approaches, defined by Wu as

researchers desire more efficient algorithms that can maximize collection and yet still avoid detection from third parties.[43] One study assessed the degree of anonymity accorded to important personal data records, including hospital and medical records. Researchers noted they could "re-identify 85% of the persons in the anonymized hospital reports using the publicly available non-personal attributes i.e. gender, age, and zip code."[44] The results showed that "simple de-identification is not enough for anonymization … and anonymization without encryption can produce false perceptions of security, causing the revelation of data meant to be confidential."[45]

While the processes embodying data collection have become more simplified through the creation of miniature storage devices designed to hold vast amounts of information, the methods have also become more complex, as scientists continue to develop state-of-the-art computer algorithms to sort through data and analyze its contents.[46] Given the ease at which large volumes of data can be stored, computer science experts have argued the wholesale recovery of all possible data across the cyber spectrum is an inexpensive and more efficient route for the federal government to separate information that is relevant to their interests and that which is irrelevant.[47] The cost of storage against the cost of having analysts

---

follows:

> (1) data hiding, in which sensitive raw data like identifiers, names, addresses, etc. were altered, blocked or trimmed out from the original database, in order for users of the data not to be able to compromise another person's privacy; (2) rule hiding, in which sensitive knowledge extracted from the data mining process be excluded for use, because confidential information may be derived from released knowledge; and (3) secure multiparty computation, where distributed data are encrypted before released or shared for computations; thus no party knows anything except for its own inputs and the results.

Id. at 762-763.

[43] *Id.* at 763.

[44] Seda Gurses et al., *PETs Under Surveillance: A Critical Review of the Potentials and Limitations of the Privacy as Confidential Paradigm* (2010), *available at* http://www.cosic.esat.kuleuven.be/publications/article-1302.pdf.

[45] *Id.*

[46] *See* MICHAEL MARCOVICI: THE SURVEILLANCE SOCIETY 3 (2013).

[47] *Id.*

survey the data results has resulted in a procedure to "record everything and sort it out later."[48] This efficiency-based mindset is typical among computer scientists, whose perceptions of privacy matters in relation to data and confidentiality have been regarded as technocentric.[49] To this end, computer scientists have promoted the static and predictable character of technology while diluting its cultural components.[50]

Today, the technologies within the current surveillance architecture are developing in a manner that has exceeded the scope of normal human faculties. Gus Hosein and Caroline Wilson Palow, two high-ranking officials at Privacy International have broken down modern surveillance technologies into three categories.[51] The first

---

[48] *Id.*

[49] *See* Gurses, *supra* note 44.

[50] *Id.* To address the power struggle between technology and individual behavior, s*ee* TIM JORDAN, HACKING: DIGITAL MEDIA AND SOCIETY SERIES 13 (2008). "Technological determinism is the claim that the nature of a particular technology determines the nature of society." *Id.* Examples cited in support of this theory include the fact that "steam energy [created] industrial society or that computers created information societies." *Id.* Hackers are the vanguard of technological deterministic theory because as a group:

> They identify where a technology is determining them in ways they dislike—from having to pay for phone calls to having email spied on—and they engage in altering that technology, which thereby automatically produces new ways in which technology can determine action.

Id. at 14-15.

[51] Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques* 74 OHIO L.J. 1071, 1080 (2013), *available at* http://moritzlaw.osu.edu/students/groups/oslj/files/2013/12/13-Hosein-Palow.pdf. These categories are identified as follows: "(1) targeted use of offensive technologies; (2) targeted and semi-targeted use of mobile-phone surveillance; and (3) mass surveillance of network activity." *Id.* at 1080-1082; *see* WILLIAM G. STAPLES, EVERYDAY SURVEILLANCE: VIGILANCE AND VISIBILITY IN POSTMODERN LIFE xii (2d ed. 2014). The author refers to the idea of "post-modern surveillance practices." *Id.* These practices consist of techniques that security agencies have used to process information inconspicuously through partnerships with cell phone and data brokerage companies. *Id.* The author delineates four characteristics of "post-modern surveillance practices:"

> 1. They are increasingly technology based, methodical, automatic, sometimes anonymously applied, and they usually generate a permanent

type of technology gives users the ability to remotely connect with a device through a computer or smartphone.[52] The technology exposes "vulnerabilities in our operating systems and applications, enabling governments to monitor all activities on the device, including all keystrokes."[53] The capability also permits the person coordinating the connection to manipulate the functional aspects of the device, including control over its microphones and cameras.[54]

The second type of technology, handheld in form, mimics a legitimate mobile communications tower, attracting phone traffic within its orbit and diverting their connections away from their intended destination and to the handheld device.[55] By pooling the mobile phones into its orbit, the device identifies the user and "enable[s] direct access to communications and metadata by routing calls through the base station."[56] In a similar context, mobile

---

record of evidence.

2. Many new techniques target and treat the body as an object that can be watched, assessed, and regulated.

3. The new techniques are often local, operating in our everyday lives.

4. Local or not, they manage to bring wide-ranging populations, not just the official "deviant" or suspect, under scrutiny.

Id. at 11.

[52] Hosein & Palow, *supra* note 51, at 1080; *see* Katina Michael & Roger Clarke, *Location and Tracking of Mobile Devices: Uberveillance Stalks the Streets*, 29 COMPUTER L. & SEC. REV. 216 (Jun. 2013), *available at* http://www.rogerclarke.com/DV/LTMD.html. The authors note the relative ease to track down a smartphone:

> During the last decade, location-tracking and monitoring applications have proliferated, in mobile cellular and wireless data networks, and through self-reporting by applications running in smartphones that are equipped with onboard global-positioning system (GPS) chipsets. It is now possible to locate a smartphone user's location not merely to a cell, but to a small area within it.

Id.

[53] Hosein & Palow, *supra* note 51, at 1080.

[54] *Id.* at 1080-81.

[55] *Id.* at 1081.

[56] *Id. See also* Pratap Chatterjee & Tom Engelhardt, *The Data Hackers: Mining Your Information for Big Brother*, OPENDEMOCRACY (Oct. 9, 2013), *available at* http://www.opendemocracy.net/pratap-chatterjee-tom-engelhardt/data-hackers-mining-your-information-for-big-brother. This particular device is known

signature devices (MDS) are used by shopping malls to both locate customers as well as gather information on their preferences in order to determine the optimal location for advertising.[57] Data surveillance scholars, Katina Michael and Richard Clarke, are wary of this method of data collection because the shoppers are unaware that data is collected and being used against them for an identified profit. [58] The information collected could lead to the exposition of more private information, including occupational data and place of residence, which are then subject to examination by the service-provider in charge of the MDS.[59]

The third type of technology concerns those devices that have tentacles in a plethora of global communications networks.[60] This

---

as an IMSI (International Mobile Subscriber Identity) catcher and is designed to "trick phones into wirelessly sending it data." *Id.* "By setting up IMSI catchers in an area and measuring the speed of responses or "pings" from a phone, an analyst can follow the movement of anyone with a mobile phone even when they are not in use." *Id.*

[57] Michael & Clarke, *supra* note 52. The authors note a company using the MDS can sense the presence of a cell phone once its signal enters its range. Once in the presence of the MDS, the device retrieves the following information:

> (1) how long each device and person stay, including dwell times in front of shop windows;
>
> (2) repeat visits by shoppers in varying frequency durations; and
>
> (3) typical route and circuit paths taken by shoppers as they go from shop to shop during a given shopping experience.

Id.

[58] *Id. See also* Chatterjee & Engelhardt, *supra* note 56. This form of tracking technology is similar to a software package developed by American military arms manufacturer Raytheon, called RIOT (Rapid Information Overlay Technology). *Id.* RIOT can "predict where individuals are likely to go next using technology that mines data from social networks like Facebook, Foursquare, and Twitter." *Id.* Raytheon describes the process as follows:

> [It] extracts location data from photos and comments posted online by individuals and analyzes this information. The result is a variety of spider diagrams that purportedly will show where that individual is most likely to go next, what she likes to do, and whom she communicates with or is most likely to communicate with in the near future.

Id.

[59] Michael & Clarke, *supra* note 52.

[60] Hosein & Palow, *supra* note 51, at 1082.

capability permits "simultaneous interception of large populations and … wide categories of information for later analysis."[61] The information then is assessed through "speaker and language recognition, mass-location tracking … keyword and topic searching, and identifying networks of individuals and groups."[62]

India's surveillance regime has also advanced in a similar direction. The development of a Unified Monitoring Centre is capable of identifying the mood of a speaker on a telephone call and take further action if, for example, the speaker sounds suspicious.[63] Other intelligence-gathering mechanisms developed by Indian companies include devices that reveal "hidden interconnections and relations through communications" as well as "advanced statistical analysis [that] can analyze more than 40 billion records in less than three seconds."[64] Furthermore, systems blanket several prominent data networks [i.e. Gmail, Hotmail, Blackberry and Yahoo], to "[correlate] identities across multiple networks, instantly analyzing data across thousands of terabytes."[65] Decoding technologies are also equipped to narrow the data pool through the use of a cell phone number, keyword, or email username.[66] Some techniques have more

---

[61] *Id. See* Glenn Greenwald & Ewen MacAskill, *Boundless Informant: the NSA's Secret Tool to Track Global Surveillance Data,* THE GUARDIAN (Jun. 11, 2013), *available at* http://cyber-peace.org/wp-content/uploads/2013/06/Boundless-Informant_-the-NSAs-secret-tool-to-track-global-surveillance-data-_-World-news-_-guardian.co_.pdf. Following the Snowden revelations, the Guardian uncovered "top secret documents about the NSA data mining tool, called Boundless Informant, that details and even maps by country the voluminous amount of information it collects from computers and telephone networks." *Id.* Reports claim 3 billion pieces of intelligence were collected by networks across the United States. *Id.* Individual users who want to inquire further into the program can "select a country on a map and view the metadata volume and select details about the collections against that country." *Id.*

[62] *Id.* at 1082-83.

[63] Maria Xynou, *Big Democracy, Big Surveillance*: *India's Surveillance State,* OPEN DEMOCRACY (Feb. 10, 2014), *available at* http://www.opendemocracy.net/opensecurity/maria-xynou/big-democracy-big-surveillance-indias-surveillance-state.

[64] *Id.*

[65] *Id.*

[66] *Id.*

widespread application within public forums [i.e. cybercafés, hotels and university campuses or free Wi-Fi zones] and expose the user's computer to harmful spyware.[67] Other methods exploit the metadata in a user's computer to monitor activity in real time.[68]

The rapid growth of sophisticated technology beckons a reevaluation of existing privacy laws, with special attention to the level of control afforded to individuals with respect to their personal information.[69] As access to greater quantities of information becomes more routine, it will behoove national governments to develop a uniform response to protect the confidentiality of sensitive data.[70] In the post-September 11th era, the problem is precisely calculating the balance between preserving the right to confidentiality over sensitive data on the one hand and the government's ability to address vital national security threats on the other.

II. Conflicting Claims, Claimants, Perspectives, and Bases of Power

A. Claims to Privacy

At its most foundational level, there is broad consensus within the social science community that privacy is a critical ingredient in a well-functioning society.[71] Defining privacy in a straightforward and coherent manner is an arduous task as the notion

---

[67] *Id.*

[68] *Id.*

[69] Michael & Clarke, *supra* note 52.

[70] *See* Hosein & Palow, *supra* note 51, at 1073.

[71] COLIN J. BENNETT: THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE 2 (2008). The omnipresent nature of the privacy interest is illustrated by a "wealth of social psychological and anthropological evidence that has suggested that every society adopts mechanisms and structures (even as simple as building walls) that allow individuals to resist encroachment from other individuals or groups." *Id.*

of privacy is multidimensional.[72] The aesthetic conception of privacy is part of what privacy advocate Colin Bennett has regarded as the "humanistic" approach to privacy issues.[73] This approach equates the absence of privacy as a "loss of human dignity … when one loses control over the circumstances under which one's space, behavior, decisions, or personal information is intruded upon."[74] The instrumental conception of privacy is based on the idea that data should be used as it was intended to be used by the "right people for the right purpose."[75] If standards are instituted to control information according to this maxim, then the expectation will be that the system can fairly and adequately process information in a reliable manner.[76]

Other commentators have argued that privacy acts as a vehicle to fulfill various values and interests.[77] Privacy scholar and former Barrister of the Supreme Court of New South Wales (Australia), Lee Bygrave offered a unique perspective on the types of values embedded within the notion of privacy. Bygrave divided these values along two separate analytical planes: those directed toward the (1) individual and (2) society as a whole.[78] As it relates to the well-being of the individual, Bygrave claims privacy gives a person the necessary space to realize his own unique identity in a stable environment that blocks out external pressures to conform to the masses.[79] In a societal construct, Bygrave argues privacy molds civil society, encouraging citizens to respect boundaries and thereby

---

[72] *Id.* at 2-3. *See also* Daniel J. Solove, *Why Privacy Matters Even If You Have Nothing to Hide*, CHRON. OF HIGHER EDUC. (May 15, 2011), *available at* https://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/. Privacy is a "plurality of different things that do not share any one element but nevertheless bear a resemblance to one another." *Id.*

[73] BENNETT, *supra* note 71, at 4.

[74] *Id.* at 5.

[75] *Id.*

[76] *Id.*

[77] *See* Lee A. Bygrave, Data Protection Law: Approaching its Rationale, Logic, and Limits (1999) (Thesis, Faculty of Law Oslo University), *available at* http://www2.austlii.edu.au/privacy/secure/Bygrave/index.html.

[78] *Id.*

[79] *Id.*

strengthening the community structure.[80] Such non-interference into the formation of opinions and habits among members in the community gives each individual an incentive to participate in the democratic process.[81] Esteemed privacy advocate Daniel J. Solove comments that government expansion has moved at an incremental pace, in which each individual intrusion undertaken by the government will in the aggregate lead to a panoptic state.[82] The evolution of the surveillance state, Solove contends, implicates a host of harms that are not inherently tangible, which complicates efforts to redress harms incurred.[83] Solove describes these harms, which include gathering small, harmless bits of data to form damaging images of the individual; denying the injured party the ability to retrieve the data; and appropriating data for extraneous purposes without the approval of the data subject.[84]

Privacy advocates[85] have emerged as a critical bulwark

---

[80] *Id.*

[81] *Id.*

[82] *See* Solove, *supra* note 72. Solove portends that the end result of an expanding government is a government that will eventually monitor every aspect of our lives. *Id. See* MICHEL FOUCAULT, DISCIPLINE & PUNISH: THE BIRTH OF PRISON 200 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977). This all-seeing or panoptic type figure is reflected in Foucault's novel. Foucault documents the mythical Panopticon described by Jeremy Bentham as a prison that "arranges spatial unities [making it] possible to see constantly and recognize immediately." *Id.* The Panopticon has the effect of "inducing in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power." *Id.* at 201. To reach a panoptic state, power should be both visible and unverifiable. *Id.* Visibility is satisfied, as "the inmate will constantly have before his eyes the tall outline of the central tower from which he is spied upon." *Id.* The fact that the inmate is being monitored should remain unverifiable: "the inmate must never know whether he is being looked at any one moment; but he must be sure that he may always be so." *Id.*

[83] Solove, *supra* note 72.

[84] *Id.*

[85] *See* Charles Raab & Bert-Jaap Koops, *Privacy Actors, Performances, and the Future of Privacy Protection*, *in* REINVENTING DATA PROTECTION? 207, 218 (S. Gutwirth et al. eds., 2009), *available at* http://www.research.ed.ac.uk /portal/files/12592176/Privacy_Actors_Performances_and_the_Future_of_Privacy _Protection.pdf. Privacy advocates include activists, academics, the media, and not-for-profit organizations. *Id.*

against public and private sector surveillance. Acting in an advisory role, privacy advocates integrate their agenda into a number of disciplines, including consumer and human rights, in order to influence policymaking on the governmental level but also on a grassroots level, through informing and educating civil society on "privacy-threatening measures."[86] Privacy activism generates its volunteer base by appealing to the negative sentiment associated with identity and tracking technologies, but is often hampered financially due to its reliance on individual donors.[87] One example of a prominent privacy organization is the Electronic Frontier Foundation (EFF).[88] The EFF claims enhancements in privacy can be realized (1) by rewarding companies who are transparent in explaining the methods behind their data transfers to the government;[89] (2) by upgrading existing laws both nationally and internationally to adjust with the rapid advancement of technology;[90] and (3) by recalibrating the balance between law enforcement needs and the preservation of individual autonomy.[91]

---

[86] *Id.* at 212.

[87] *Id.* at 218.

[88] *About EFF*, ELECTRONIC FRONTIER FOUNDATION, *available at* https://www.eff.org/about. (last viewed Feb. 13, 2014). The EFF serves as a defender of the "public interest in every critical battle affecting digital rights." *Id.* The EFF's mission is described as follows:

> [EFF confronts] cutting-edge issues defending free speech, privacy, innovation, and consumer rights. Blending the expertise of lawyers, policy analysts, activists, and technologists…EFF fights for freedom primarily in the courts, bringing and defending lawsuits even when that means taking on the U.S. government or large corporations.

Id.

[89] Marcia Hoffman, *Who Has Your Back? 2013*, ELECTRONIC FRONTIER FOUNDATION (Apr. 30, 2013), *available at* https://www.eff.org/wp/who-has-your-back-2013. The EFF carried out a comprehensive study into the "policies of major internet companies — including ISPs, email providers, cloud storage providers, location-based services, blogging platforms, and social networking sites"—as a litmus test of their allegiance to the user when the government wants certain information. *Id.*

[90] *Privacy*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/privacy (last viewed Feb. 13, 2014).

[91] *Id.* EFF claims domestic law should create a more enhanced system of checks and balances to prevent abuses of state of power, while "international

EFF has claimed the state's decision to pursue data collection policies threatens the individual's right to associate with others.[92] In its representation of advocacy groups affected by government surveillance, EFF has argued that government access to phone records is an impediment to activist groups, who are concerned over the government's ability to extract information from those records to determine the composition of its membership and the content of conversations among members.[93] EFF has warned that this capability is a recipe for not only targeting specific individuals who frequent organizations regularly, but also for uncovering that person's connections with other like-minded individuals.[94] The EFF has concluded that such unfettered access would create a "chilling effect" and deter individuals from affiliating with organizations.[95]

The American Civil Liberties Union (ACLU) has argued against warrantless surveillance on the grounds that the government is constitutionally obligated under the Fourth Amendment to do its due diligence before it searches any individual, specifically through "evidence demonstrating that there exists strong reason (enough to convince a judge) for believing that [a] particular person is likely to be a criminal or a terrorist."[96] Once that requirement is satisfied, they argue, a person can be the object of surveillance.[97] Civil Libertarians claim that even if the presence of government surveillance poses minimal harm, "the infrastructure is in place for a less benevolent leader to violate the people's rights and set [the nation] on the path to tyranny."[98]

---

bodies need to consider how a changing technological environment shapes security agencies' best practices."

[92] *NSA Spying on Americans*, ELEC. FRONTIER FOUND., *available at* https://www.eff.org/cases/first-unitarian-church-los-angeles-v-nsa. (last viewed on Feb. 13, 2014).

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] Amitai Etzioni, *NSA: National Security vs. Individual Rights*, INTELLIGENCE & NAT'L SECURITY 14 (Jan. 24, 2014), *available at* http://dx.doi.org/10.1080/02684527.2013.867221.

[97] *Id.* at 14-15.

[98] *Id.* at 35.

B. Counterclaims to the Privacy Right

1. Privacy is not a Universal Value

Whereas privacy advocates maintain that the right to privacy should be accorded special recognition, some schools have not accepted the existence or desirability of such a right. Cultural relativists associate the concept of privacy with the West and argue "many countries and cultures can choose to ignore privacy rights in [favor] of group rights, the needs of the public, and the needs of the state."[99] Reductionists argue against a right to privacy "because any interest protected by the right to privacy can be equally well explained and protected by other interests or rights, most notably the rights to property and bodily security."[100] Technological defeatists[101] rely on a dystopian view arguing that despite the existence of privacy values, the pursuit toward safeguarding privacy is pointless because of the continued growth in surveillance capabilities.[102] In the realm of e-commerce, businesses and data controllers have addressed the concerns of privacy interference by highlighting the tangible benefits received by individuals from continuous data processing.[103] By

---

[99] Gus Hosein, *Privacy and Developing Countries*, OFFICE PRIVACY COMM'R CAN. (Sep. 2011), *available at* https://www.priv.gc.ca/information/research-recherche/2011/hosein_201109_e.asp.

[100] ALEXANDRA RENGEL, PRIVACY IN THE 21ST CENTURY 36 (2013) (citing Judith Jarvis Thomson, *The Right to Privacy*, 4 PHILOSOPHY & PUB. AFF. 295, 306 (Summer, 1975)).

[101] *See* Evgeny Morozov, *The Wrong Way to Discuss New Technologies*, SLATE (Mar. 7, 2013), *available at* http://www.slate.com/articles/technology/future_tense/2013/03/to_save_everything_click_here_how_to_vanquish_technological_defeatism.html. The doctrine of technological defeatism encourages society to surrender to a particular technology. *Id.* Adherents state "we can choose to modify our legal and political and economic assumptions to meet the ordained [technological] trajectories ahead. But we cannot escape from them." *Id.*

[102] *See* Froomkin, *supra* note 10, at 1539. Froomkin cites futurist David Brin, who argued that the "time for privacy laws passed long before anyone noticed." *Id.* Brin contended "it is already far too late to prevent the invasion of cameras and databases … [n]o matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases." *Id.*

[103] *See* Jules Polonetsky & Omar Tene, *Privacy and Big Data: Making Ends*

collecting information from the individual, businesses argue their ability to provide a customized[104] atmosphere for the online user improves protection from unwarranted threats[105] and expedites the user's search capabilities.[106] Furthermore, businesses argue greater quantities of data help "[o]ptimize distribution methods, efficiently allocate credit, and robustly combat fraud," which in turn positively affects the consumer.[107] The overarching interest therefore among data handlers is to reassure data subjects that their information is properly supervised and used responsibly.[108]

2. Privacy should defer to needs of national security

National security proponents have argued the aims of the intelligence community cannot coexist with efforts to make the system more transparent to the public.[109] This view warns of the emergence of movements aimed at weakening government efforts to strengthen homeland security.[110] Others have noted that

---

Meet, 66 STAN. L. REV. ONLINE 25 (Sep. 3, 2013), *available at* http://www.stanfordlawreview.org/online/privacy-and-big-data/privacy-and-big-data.

[104] *Id.* The authors discuss efforts by Netflix and Amazon to use data as a way to "[r]ecommend films and products to consumers based on analysis of their previous interactions." *Id.*

[105] *Id.* Internet providers are known to have contacted consumers over malware threats and have even checked in on their customers' computers to detect the threat. *Id*.

[106] *Id.* Google has also employed "[a]utocomplete and translate functions based on comprehensive data collection and real time keystroke-by-keystroke analysis." *Id*.

[107] *Id.*

[108] Bygrave, *supra* note 77.

[109] Gerald Walpin, Former Inspector General under George W. Bush, *We Need NSA Surveillance,* NAT'L REV. ONLINE (Aug. 16, 2013), *available at* http://www.nationalreview.com/article/355959/we-need-nsa-surveillance-gerald-walpin.

[110] *Id.* In supporting the government's position, Walpin refers to Federalist Papers No. 23 which reads as follows:

> The Government's "powers" for the "common defense … ought to exist without limitation *because it is impossible to foresee or define the extent and variety of national exigencies, or to the correspondent extent and*

modernization through technological innovation has led to the formation of a risk society.[111] When risk arises, surveillance acts as a tool to manage the hazards flowing from modernization.[112] These hazards are aligned around three major hotspots: "ecological, global financial and global terror networks."[113] Risk theorists believe a prudent strategy that acknowledges and neutralizes the source of the problem in a discrete manner is an effective way to counter the aforementioned security threats.[114] In the case of the NSA's data collection programs, the NSA and the Obama Administration have argued the programs are critical in the current campaign against terrorism.[115] Specifically, the programs give insight into terrorist networks and aid counter-terrorism officials in the identification of suspected terrorists and their contacts overseas.[116]

variety of the means which may be necessary to satisfy them."

Id.

[111] ERIC STODDART, THEOLOGICAL PERSPECTIVES ON A SURVEILLANCE SOCIETY-WATCHING AND BEING WATCHED 103 (2011).

[112] *Id.*

[113] *Id.* at 104.

[114] *Id.* at 103.

[115] David Jackson, *Government Officials Defend Phone Surveillance Program*, USA TODAY (Jun. 6, 2013), *available at* http://www.usatoday.com/story/news/politics/2013/06/06/obama-verizon-phone-records-guardian-story-privacy-terrorism/2395695/.

[116] *Id.*

III. Past Trends in Decisions and Their Conditioning Factors

A. United States

The United States is a liberal democracy emphasizing restraint on government power.[117] Due to the diversity of viewpoints existing among a population of 300 million and the heavily bureaucratic nature of the American government,[118] the issue of information privacy resurfaces time and time again on the American political landscape.[119] Commentators have labeled data privacy regulation as "fragmented,[120] ad hoc, and narrowly targeted to cover

---

[117] *See* SEYMOUR MARTIN LIPSET, CONTINENTAL DIVIDE: THE VALUES AND INSTITUTIONS OF THE UNITED STATES AND CANADA (1990). The United States stands in direct opposition to Machiavellian principles, namely the power of the prince. *Id.* at 20. Instead, the U.S. Constitution "[provides] for an elaborate system of checks and balances." *Id.* at 21. Moreover, the "The American Constitution with its Bill of Rights emphasizes due-process guarantees for the individual and limits on state power." *Id.* at 50.

[118] Panagiotis Grigoriou, *Bureaucracy: Administrative Structure and a Set of Regulations in Place to Control Organizational or Governmental Activities*, *available at* http://www.balcannet.eu/materiale/research2.pdf. (last visited Nov. 6, 2013). "Bureaucracy is the administrative structure and set of regulations in place to control … activities, usually in large organizations and government." *Id. at* 1. It is characterized by hierarchical relations, in which officials have the "tendency to behave extra-constitutionally and act beyond ethical framework that guards and guides its official conduct." *Id.*at 2. Since the expansion of government necessitates "well-trained officials to administer and manage the complexity … [of the] government's business … [the] government employs unprecedented numbers of people to deal with an unprecedented range of tasks and [specialization.]" *Id.* at 3. The fact that these people assigned with the responsibility of administering government duties are "non-elective officials" and can exert "control over the national administration and economy" makes any contribution by the people or elected representatives difficult. *Id.*

[119] Alan F. Westin, *Social and Political Dimensions of Privacy*, 59 J. SOC. ISSUES 2, 5 (2003). The privacy issue is a recurring phenomenon because "[i]t involves the proper roles of government, the degree of privacy [afforded to] sectors such as business, science, education, and the professions, and the role of privacy claims in struggles over rights such as equality, due process, and consumerism." *Id.*

[120] McKay Cunningham, *Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law*, 44 GEO. WASH. INT'L L. REV. 643, 664 (2012).

specific sectors and concerns."[121] Moreover, the lack of an overarching privacy law directed by a single governing authority, a byproduct of the American federalist[122] system, has complicated the

---

Special attention should be noted to the entertainment industry which aptly reflects the fragmented state of data regulation in the United States: there are three separate statutes (Cable Communications Policy (CCPA) of 2006, Telecommunications Act of 1996, and Video Privacy Protection Act (VPPA) of 1998 "[regulating the] use of name and address information depending on whether the subscription is for cable television, telephone service, or video rental." *Id.*

[121] Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of US Data Privacy Regulations*, 25 YALE J. INT'L L. 1, 22 (Winter, 2000); *see Ponemon and Symantec Find Most Data Breaches Caused by Human and System Errors*, SYMANTEC (2013), *available at* http://www.symantec.com/about/news/release/article.jsp?prid=20130605_01. The potential for data breaches are found "within heavily regulated fields, including healthcare, finance, and pharmaceutical." *Id.* These industries "incurred breach costs 70 percent higher than other industries." *Id;* Cunningham, *supra* note 39, at 664. Data protection legislation imposes burdens on industries that "handle sensitive private data and the laws are often narrowly tailored addressing particular elements of personal information or discrete uses of discrete data." *Id.*

[122] MARKKU SUKSI, SUB-STATE GOVERNANCE THROUGH TERRITORIAL AUTONOMY: A COMPARATIVE STUDY IN CONSTITUTIONAL LAW OF POWERS, PROCEDURES, AND INSTITUTIONS 126-27 (2011). Although no established theory on federalism exists, there are two elements of a federation that can be contrived:

> [First,] the federal legislative body is organized so as to provide for equal (or sometimes less than equal) representation for the constituent or component states of the federation in one chamber of the federal legislature, elected or appointed, while the other chamber is normally directly elected by the inhabitants of the constituent or component states in a way which guarantees the proportional representation of the population… [s]econd, at least in a federation of the classical model, the federal legislature and the central authorities have enumerated powers, which means they are in the possession of specific jurisdictional competences or certain specified functions which, at least in theory, have been granted to the federation by the constituent entities. Constituent states, in turn, remain in possession of residual jurisdictional competencies, which allows the characterization of the basis of their powers as a general competence. Hence, the constituent states are empowered to deal with all matters not explicitly reserved to the federal level…[T]he idea underpinning the distribution of powers between the federal and state levels in a federation … is that the constituent states have retained at least some traces of their original sovereignty, albeit in a way profoundly circumscribed by the federation.

level of enforcement for data breaches.[123] The United States focused its attention on information privacy starting in the 1960s as both the government and private sector contemplated an approach toward streamlining the record-keeping and storage of federal data.[124] Increased information inflow into federal agencies[125] necessitated a more efficient method to make data more accessible[126] to the American public. Instead of having each government agency operate its own record-keeping system, by 1965, the Social Science Research Council[127] submitted a proposal calling for the creation of a

---

Id.

[123] Dorothy Glancy, *At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH L.J. 357, 378 (2000). Privacy law in the United States is composed of both state and federal law. *Id.* At times provisions within state and federal law coexist with "private sector representations regarding privacy policies and industry privacy standards." *Id.* Intermingling state and federal law has a noticeable effect on the electronic surveillance regime. *Id.* at 379. For example, one difficulty in carrying out the objectives of the ECPA is the fact the federal underbelly of the statute does not override state statutes that offer greater privacy protection, which envisions the scenario of one individual being prosecuted for wiretapping a phone line under California's privacy-friendly privacy laws versus an individual committing the same act in New Hampshire, which recognizes forms of electronic eavesdropping. *Id.* at 379-380.

[124] *See Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400, 401 (1968) [hereinafter *Privacy and Efficient Government*], *available at* http://simson.net/ref/1966/Harvard_Law_Review_article_on_National_Data_Center.pdf.

[125] *Id.* at 402. The proposal for the National Data Center took into account the potential input of "9,000 reels of representative data principally from … the Bureau of Census ([consisting of] population and housing data), the Bureau of Labor Statistics, the Internal Revenue Service, and the Social Security Administration." *Id*.

[126] *Id.* Accessibility to basic information propelled the idea for a National Data Center. *Id.* However, this objective was tempered by the need to "[develop] safeguards for preserving the privacy of personal disclosures to the government … and [minimizing] the burden upon citizens and institutions called on to furnish information." *Id*.

[127] *See* Kenton W. Worcester, *Social Science Research Council: 1923-1998*, SOC. SCI. RESEARCH COUNCIL (2001), *available at* https://s3.amazonaws.com/ssrc-cdn1/crmuploads/new_publication_3/%7B1F20C6E1-565F-DE11-BD80-001CC477EC70%7D.pdf. The Social Science Research Council became the "world's first national organization of all the social sciences, and from the outset

centralized database known as the "National Data Center"[128] to pool data from various agencies.[129] The proposal did not gain much traction in the United States Senate,[130] among other reasons,[131]

---

its goal has been to improve the quality of, and infrastructure for, research in the social sciences." *Id.* at. 15.

[128] Rebecca S. Kraus, *Statistical Déjà Vu: The National Data Center Proposal of 1965 and Its Descendants*, U.S. CENSUS BUREAU (Aug. 1, 2011), *available at* http://www.census.gov/history/pdf/kraus-natdatacenter.pdf. The National Data Center was advanced by the social science community as a way to "preserve data collected by its agencies and make the data available to researchers both within and outside the government." *Id.* at 7. The purpose of the National Data Center would be to "provide user services and basic information about the U.S. economy." *Id.* at 8. Under the proposal, "[the National Data Center] would have the authority to obtain computer tapes produced by other agencies" and "provide aggregate data or results to scholars*." Id.*

[129] JAMES P. NEHF, OPEN BOOK: THE FAILED PROMISE OF INFORMATION PRIVACY IN AMERICA 37 (2012), *available at* http://ssrn.com/abstract= 2192471; *see Privacy and Efficient Government*, *supra* note 121, at 400. Another factor prompting the creation of the Data Center was to "take fuller advantage of modern technology by centralizing the federal statistical network." *Id.*

[130] Kraus, *supra note* 128, at 16. The author chronicles the events that led to the eventual demise of the Federal Data Center:

> At first, congressional concern was focused on the impact of technological change on individual privacy. However, concern soon turned to the extent of information on individuals maintained by federal agencies. In 1966, the Senate Subcommittee on Administrative Practice and Procedure surveyed federal agencies about the amount of personal information they collected. The study identified more than three billion records on individuals, including names, addresses, criminal histories, mental health records, and financial records … [concluding] that much of the information collected by the government was irrelevant and in some instances, confidentiality provisions were not meaningful or not enforced.

Id. at 16-17.

[131] *Privacy and Efficient Government*, *supra* note 124, at 411-12. The "Data Center created some concerns:

> statistical data could be used or misused by overzealous government officials; … improved capacity for data handling might result in requests by government agencies for new and more personal data; … [increased] reliance on computers to make decision [would] vitally affect human interests; … people would so fear the possibility of exposure of their data files that they would "act for the record" with a consequent increase in conformity.

Id.

because of its potential for fueling government intrusiveness.[132]

1. Formative Years of the Privacy Discourse

The debate over the extent to which the government can access data and the communications of the population reached a pivotal juncture in 1967, with the decision in *United States v. Katz.*[133] In *Katz,* the Supreme Court ruled that wiretapping and other flavors of electronic surveillance undertaken in a standard criminal case were searches within the confines of the Fourth Amendment.[134] Following the *Katz* decision, in 1968, Congress promulgated Title III of the Omnibus Crime Control and Safe Street Acts of 1968.[135] Title III applied the standard procedures employed in obtaining search warrants for warrants seeking electronic surveillance.[136] However, Title III permitted law enforcement to disseminate information

---

[132] *Id.* at 416; *see* Kraus, *supra note* 128, at 18. The National Data Center induced fear of "loss of privacy, infringement of rights, and even totalitarianism." *Id.* A number of prominent newspapers across the United States expressed unfavorable sentiments to the National Data Center with the following headlines:

"Tyranny of the Statistic," *Christian Science Monitor*, July 29, 1966

"Computer Abuse Threatens Privacy," *Systems*, September 1966

"Computer as Big Brother," *Pittsburgh Post-Gazette*, August 1966

"Big Brother Never Rests," *Indianapolis Star*, August 15, 1966

"A Giant Peeping Tom," *Paterson (NJ) Evening News*, August 8, 1966.

Id.

[133] *See* United States v. Katz, 389 U.S. 347 (1967).

[134] *Id.* at 358-359. The court noted that fourth amendment considerations "do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth." *Id*.

[135] Richard A. Posner, *Privacy, Surveillance, and the Law*, 75 U. CHI. L. REV. 245, 251 (2008); *see also* Eric Rosenbach & Aki J. Peritz, *Electronic Surveillance and FISA: Memorandum in Report, Confrontation or Collaboration? Congress and the Intelligence Community*, BELFER CTR. SCI. & INT'L AFF. (July 2009). Rosenbach describes Title III as one of the two main frameworks of electronic surveillance; the other being the Foreign Intelligence Surveillance Act of 1978. *Id.* Title III "covers surveillance in the investigation of serious domestic crimes." *Id.*

[136] Posner, *supra* note 135, at 251 (citing Nicholas J. Whilt, *The Foreign Intelligence Surveillance Act: Protecting the Civil Liberties That Make Defense of Our Nation Worthwhile*, 35 S.W. U. L. REV. 361, 371 (2006).

derived from surveillance authorized by Title III if "the information is of overriding importance to national security or foreign relations and disclosure is necessary for the President to discharge his constitutional responsibilities over these matters."[137]

In 1970, Congress passed the Fair Credit Reporting Act (FCRA)[138] to hold credit reporting agencies accountable for protecting the confidentiality of consumer information.[139] Congress discovered that individuals were "rendered virtually unemployable or who had been refused credit on the basis of inaccurate and damaging reports."[140] One of the aims of the FCRA was to set parameters for information requests, keeping such inquiries limited to business related matters.[141] In an attempt to increase transparency, the FCRA mandated the implementation of "reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates."[142] Foreseeing the

---

[137] DEP'T OF JUSTICE OFFICE OF INTELLIGENCE AND POLICY REVIEW: SHARING TITLE III ELEC. SURVEILLANCE WITH THE INTELLIGENCE COMMUNITY-MEMORANDUM FOR THE COUNSEL (Oct. 17, 2000), *available at* http://www.justice.gov/olc/titleIIIfinal.htm. From the language of Title III and the ambiguity attached to matters connected with national security, the Executive possessed wide latitude to justify its collection of data. (emphasis added).

[138] *See* 15 U.S.C. § 1681(b).

[139] Sheldon Feldman, *The Fair Credit Reporting Act*: *From the Regulators Vantage Point*, 14 SANTA CLARA L. REV. 459, 459 (1974). The "consumer reporting industry" up until the passage of the FCRA "operated almost entirely outside the scrutiny of state and federal regulators and functioned without the need or desire to involve consumers in its operations." *Id.* at 461.

[140] *Id*. at 459.

[141] *Id.* at 463.

[142] *Id*. at 463. The FCRA created several basic rights including:

> a) notification of adverse action to allow the aggrieved party to correct any erroneous information in the file; b) right to access file to learn the "nature and substance" of the information in the file; c) right to be told the sources and recipients of information except that the sources of information acquired solely for use in preparing investigative reports need not be disclosed except under appropriate discovery procedures in court; d) right to have information held confidential subject to court order or at the direction of the consumer; e) right to have consumer reporting agencies reinvestigate disputed items of information and correct inaccurate items. f) right to have agencies to assure that recipients of the

growth in computerized information and its societal impacts, the U.S. Department of Health, Education, and Welfare (HEW),[143] in 1973, published a report entitled "Records, Computers, and the Rights of Citizens."[144] The report recognized a movement led by state and federal governments toward data centralization and envisaged a new set of rights in the area of privacy protection.[145]

> reports certify that they are authorized to receive them; g) right to not have adverse information reported if older than seven years…the agency must notify the consumer when adverse public record information is being reported to a potential employer and re-verify the information after three months; h) right to have those who procure or request investigative consumer reports to inform the consumer in writing (a) that such investigation may be made… and (b) that the consumer has the right to make a written request for disclosure of the nature and scope of the investigation; i) right to bring a civil suit for willful noncompliance with the Act and sue for actual damages.

Id. at 463-466.

[143] *A Common Thread of Service: A Historical Guide to HEW*, U.S. DEP'T HEALTH & HUM. SERV. (Jul. 1, 1972), *available at* http://aspe.hhs.gov/info/hewhistory.htm. HEW was created on April 11, 1953 with an objective to improve the administration of Federal responsibilities in the fields of health, education, and social security. *Id.*

[144] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 127-128 (2004). The report on "Records, Computers, and Rights of Citizens" and its accompanying Code of Information Practice provided a blueprint towards integrating all participants, both public and private, in establishing a privacy framework. *Id.*

[145] NEHF, *supra* note 129, at 38 n.103. The Code of Information Practices, which concluded the "Records, Computers, and the Rights of Citizens" report states that:

> a) There must be no personal record-keeping system whose very existence is secret.
>
> b) There must be a way for an individual to find out what information is in a record and how it is used.
>
> c) There must be a way for an individual to prevent information about him or her that was obtained for one purpose from being used or made available for other purposes without his or her consent.
>
> d) There must be a way for an individual to correct or amend a record of identifiable information about him or her.
>
> e) All organizations creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of

Despite the HEW report, by 1974, no concrete mechanism existed within the United States to slow the government's growing technological capacity to penetrate individual privacy.[146] The Watergate Scandal,[147] however, pushed Congress "[to curb] the illegal surveillance and investigation of individuals by federal agencies."[148] Congress pressed for the implementation of a fair information practices code that would help safeguard against potential federal misuse of social security numbers to gain access into personal files.[149] The Privacy Act of 1974 (Privacy Act)[150] answered the call for reform by according individuals due process rights[151] against the federal government's use and dissemination of

---

data.

Id.

[146] *The Privacy Act of 1974*, ELEC. PRIVACY INFO. CTR. *available at* http://epic.org/privacy/1974act/ (last visited Oct. 23, 2013) [hereinafter *Privacy Act of 1974*]; *see* James Beverage, *The Privacy Act of 1974*: *An Overview*, 1976 DUKE L.J. 301, 301 (1976). A measure was needed to protect the individual because "the executive branch had no general policy governing data collection and use and judicial action by its nature tended to be more remedial than preventative." *Id.*

[147] *Watergate: The Scandal that Brought Down Richard Nixon*, WATERGATE.INFO, *available at* http://watergate.info/ (last viewed Feb. 22, 2014). Watergate is a reference to a series of scandals that occurred during the Nixon Administration from 1972 to 1974. *Id.* However, the break-in at the Watergate Hotel in Washington D.C. was the main event—burglars broke into the main office complex of the Watergate Hotel and bugged the Democratic Party's National Committee offices. *Id. See Brief Timeline of Events*, WATERGATE.INFO, *available at* http://watergate.info/chronology/brief-timeline-of-events (last viewed Feb. 22, 2014). Eventually, some of Nixon's aides were prosecuted for conspiracy, burglary, and wiretapping of conversations. *Id.*

[148] U.S. JUSTICE DEP'T OFFICE OF PRIVACY AND CIV. LIBERTIES: OVERVIEW OF THE PRIVACY ACT OF 1974 4 (2012), *available at* http://www.justice.gov/opcl/1974privacyact-2012.pdf.

[149] *Id.*

[150] Jerome J. Hanus & Harold C. Relyea, *A Policy Assessment of the Privacy Act*, 25 AM. U. L. REV. 555, 557 (Spring, 1976). The Privacy Act obligates the federal government "to give notice of the record systems it establishes, restricts intra government transfer of personally identifiable records, and ensures a data subject's access to his own records." *Id.* at 573.

[151] Julianne M. Sullivan, *Will the Privacy Act of 1974 Still Hold Up in 2004? How Advancing Technology Has Created a Need for Change in the "System of Records" Analysis,* 39 CAL. W. L. REV. 395, 397 (Spring, 2003). The Privacy Act

personal information.[152] However, the Privacy Act contained loopholes for regulatory compliance, especially for federal agencies, including the CIA and FBI.[153] Moreover, it crafted a provision for "routine use"[154] which gave the government interpretative freedom to justify a particular disclosure.[155]

2. Enter FISA and the Expansion of Electronic Surveillance

Following President Nixon's resignation, Congress took precautionary measures to address growing concerns over the Executive Branch's ability to conduct surveillance not only on targets overseas but also on what the government perceived were domestic agitators.[156] Before the United States Senate Select Subcommittee to Study Governmental Operations with Respect to Intelligence Activities (Church Committee),[157] testimony revealed

---

addresses several key issues:

> [It protects] individuals' private information from disclosure by government agencies that have collected it, and [enables] individuals to determine what information has been collected … to verify its accuracy. [Moreover, it] provides a mechanism for individuals to challenge their records and request corrections of the data stored by the agency, and a remedy against those who do not comply.

Id.

[152] 5 U.S.C. § 552a (e) (6) (1974).

[153] Michael McFarland, Scholar at Santa Clara University Markkula Center for Applied Ethics, *Privacy and the Law* (2012), *available at* http://www.scu.edu/ethics/practicing/focusareas/technology/internet/privacy/privacy-law.html.

[154] 5 U.S.C § 552a (7) (1974). Routine use refers to "with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected." *Id.*

[155] McFarland, *supra* note 153.

[156] *See* Stephen Bradbury, Former Head of the Office of Legal Counsel of the U.S. Department of Justice 2005-2009, *Understanding the NSA Programs Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targeted Collection Under Section 702*, 1 LAWFARE RES. PAP. SER. 1, 15 (Sep. 1, 2013), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/Bradbury-Vol-1-No-3.pdf.

[157] *See* Frederick A.O. Schwarz, Jr. *The Church Committee, Then, and Now,*

the CIA committed various abuses, which included monitoring anti-war activists and collecting information on American citizens.[158] To ensure proper judicial oversight of intelligence activities, Congress in collaboration with the President and Justice Department ushered in the Foreign Intelligence Surveillance Act of 1978 (FISA).[159] As discussed in its preliminary stages, lawmakers desired greater

---

in US NATIONAL SECURITY, INTELLIGENCE, AND DEMOCRACY: FROM THE CHURCH COMMITTEE TO THE WAR ON TERROR 22, 22 (Russell A. Miller ed., 2008). Schwarz, Jr. asserts the Church Committee's investigation was pivotal in the following ways:

> First, it exposed in great detail decades of conduct at home that was inconsistent with American ideals, that violated the Constitution and the law, and that often was a diversion from more important objectives. Second, it revealed conduct abroad that was inconsistent with a "decent respect [for] the opinions of mankind" (to borrow a phrase from the Declaration of Independence) as well as often being harmful to America's long-term interests… [I]n addition the facts exposed by the committee stand as an object lesson of how, over the course of decades, secrecy, inadequate—or non-existent—oversight, and vague, fuzzy laws lead to abuse, excess, and foolishness.

Id. at 22-25.

[158] *See* Gary Hart, *Liberty & Security*, *in* US NATIONAL SECURITY, INTELLIGENCE, AND DEMOCRACY: FROM THE CHURCH COMMITTEE TO THE WAR ON TERROR 13, 20 at n.18 (Russell A. Miller ed., 2008). Hart recalls Seymour Hersh in his article *Underground for the C.I.A. in New York: An Ex-Agent Tells of Spying on Students,* N.Y. TIMES (Dec. 29, 1974). It was revealed that "files on over ten-thousand American citizens had been compiled by the agency, despite the language of the 1947 act that barred the CIA from any security or police function within the United States." *Id.*

[159] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. § 1801, *et. seq.*). *See also* Rosenbach, *supra* note 135. FISA's role would be served in the following ways:

> [1] FISA would be the "exclusive means" governing the use of electronic surveillance in international terrorism and other foreign intelligence investigations.
>
> [2] The Federal Bureau of Investigation (FBI) and [National Security Agency (NSA)] would serve as the lead agencies to gather foreign intelligence relevant to the FISA framework
>
> [3] The [intelligence community] would work through the Foreign Intelligence Surveillance Court (FISC) to secure a warrant before undertaking foreign intelligence surveillance of a domestic nature.

Id.

supervision over foreign intelligence activities conducted by agencies established by Congress.[160] To assess the validity and legality of surveillance obtained by these agencies, FISA established a Foreign Intelligence and Surveillance Court (FISC) to authorize the issuance of warrants in connection with national security investigations.[161] An impartial magistrate reviews and approves surveillance activities conducted for foreign intelligence purposes when the proposed surveillance could implicate the Fourth Amendment rights of any U.S. person.[162] The FISC operates clandestinely[163] in a one-sided proceeding attended exclusively by the Department of Justice.[164] Moreover, FISC judges give great deference to the government's certification that the facts and circumstances presented support an order unless the government's claims are "clearly erroneous."[165]To obtain a warrant for a specific surveillance measure, FISA set forth a lower threshold for the traditional probable cause requirement defined in Title III.[166] Whereas in Title III, there must be probable cause to believe a given circumstance will reveal the fruits of criminality, under FISA the government must show a "significant purpose of the surveillance is

---

[160] *See* Foreign Intelligence Surveillance Act of 1978, H. Rept. No. 95-1283, Pt. I, 95th Cong., 2d Sess. 15 (1978).

[161] *Foreign Intelligence Surveillance Court*, ELEC. PRIVACY INFO. CTR., *available at* http://epic.org/privacy/terrorism/fisa/fisc.html. (last visited Feb. 22, 2014).

[162] *See* Laura K. Donahue, *Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing Before the S. Committee on the Judiciary, 113th Congress*, GEORGETOWN U. L. CTR. 17 (Oct. 2, 2013), *available at* http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1117&context=cong.

[163] *See* Nola K. Breglio, *Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance*, 113 YALE L.J. 179, 189 (2003). This clandestine character is exemplified by the difficulty in even getting an appeal "since a defendant might never know such an order had existed in his case or what proof the government had submitted in support of it." *Id.*

[164] Matt Bedan, *Echelon's Effect: The Obsolescence of the U.S. Foreign Intelligence Legal Regime*, 59 FED. COMM. L.J 425, 432 (2007), *available at* http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1477&context=fclj.

[165] Mayfield v. United States, 504 F.Supp.2d 1023, 1039.

[166] Breglio, *supra* note 163, at 203.

to obtain foreign intelligence information."[167] This purpose statement does not give criteria on the category of crimes that can be heard before the FISC.[168] Furthermore, the federal official must include in the application, among other items, that the "target of the surveillance is a foreign power or agent of a foreign power and that each of the facilities or places at which electronic surveillance is directed (or about to be) used by a foreign power or an agent thereof."[169] When the application is approved, FISA enforces a minimization process to discard any privileged, extraneous material not within the scope of the targeted surveillance.[170] However, commentators have noted this process occurs following a FISA-authorized collection.[171]

During the early years of FISA, the Supreme Court heard the

---

[167] 50 U.S.C. § 1804 (a) (6) (A)-(B); *see* Charles Doyle, Senior Specialist in the American Law Division, *The USA Patriot Act: A Legal Analysis*, CONG. RESEARCH SERVICE 8 (Apr. 15, 2002), *available at* http://assets.opencrs.com/rpts/RL31377_20020415.pdf. The parameters of the "purpose" requirement have been the subject of litigation since the purpose requirement was included in the initial drafting of FISA. *Id. "*Defendants often questioned whether authorities had used a FISA surveillance order against them in order to avoid the predicate crime threshold for a Title III order." *Id.*

[168] Scott J. Glick, *FISA's Significant Purpose Requirement and the Government's Ability to Protect National Security,* 1 HARV. NAT'L SECURITY J. 87, 102 (May 30, 2010), *available at* http://harvardnsj.org/wp-content/uploads/2010/05/Vol.1_Glick_Final.pdf.

[169] Donahue, *supra* note 162, at 17. The applicant must also outline:

> the identity of the Federal officer making the application, the identity, if known, of the target, a statement of the facts and circumstances relied upon to justify the applicant's belief that the target is a foreign power or an agent of a foreign power … a statement of the proposed minimization procedures, a description of the nature of the information sought, a certification from an executive branch official, a summary statement of the means by which the surveillance will be effected, a statement of the facts concerning all previous applications, and a statement of the period of time for which the surveillance will be maintained.

Id. at 18.

[170] *See* Rosenbach, *supra* note 135.

[171] *Id. See also* In Re All Matters, FISA Ct. (May 2002), *available at* https://www.fas.org/irp/agency/doj/fisa/fisc051702.html. "Virtually all information seized, whether by electronic surveillance or physical search, is minimized hours, days, or weeks after collection." *Id.*

landmark case of *Smith v. Maryland*,[172] to determine whether a coordinated effort by police to have a telephone company use a pen register[173] without warrant to log numbers dialed from the petitioner's home violated the petitioner's reasonable expectation of privacy.[174] The court determined that pen registers do not gather the contents of communications but only the numbers that are dialed.[175] Since the petitioner, like other telephone users, willingly transferred his phone number to the telephone company and could foresee the possibility of disclosure, his legitimate expectation of privacy vanished.[176] By 1986, Congress passed the Electronic

---

[172] *See generally*, Smith v. Maryland, 442 U.S. 735 (1979).

[173] *See* 18 U.S.C. § 3127(3). The statutory definition of a pen register is listed as follows:

> "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, *provided however*, that such information shall not include the contents of any communication…

Id. (emphasis added).

[174] Smith, 442 U.S. at 738.

[175] *Id.* at 741. The discussion *infra* Part III.A(3) regarding Section 215 and bulk collection of metadata seems to reaffirm the holding in Smith and strengthen the NSA's argument that its programs have proper legal backing despite the heavy wave of criticism by privacy advocates. However, *see* Daniel Solove, *Reconstructing Electronic Surveillance Law,* 72 GEO. WASH. L. REV. 1701, 1726-1727 (2004). The distinction between content and non-specific information is a vexing issue especially when considering pen registers, email, IP addresses, and URLs. *Id.* To illustrate this issue, Solove discusses IP addresses:

> An IP address is a unique number that is assigned to each computer connected to the Internet. Each website, therefore, has an IP address. On the surface, a list of IP addresses is simply a list of numbers; but it is actually much more. With a complete listing of IP addresses, the government can learn quite a lot about a person because it can trace how that person surfs the Internet. The government can learn the names of stores at which a person shops, the political organizations a person finds interesting…and so on.

Id. at 1727.

[176] Smith, 442 U.S. at 744. The Smith court followed the reasoning espoused in United States v. Miller 425 U.S. 435, 442 (1976), in which "a bank depositor had no 'legitimate expectation of privacy' in financial information voluntarily conveyed to … banks and exposed to their employees in the ordinary course of

Communications Privacy Act (ECPA).[177] The ECPA has several functions, which include "[outlawing] unauthorized interception of wire, oral, or electronic communications [as well as] establishing a judicially supervised procedure to permit such interceptions for law enforcement purposes."[178] However, the ECPA did not modify its original provisions to account for the various layers of complexity associated with advances in technology.[179] In its present form, the federal government can issue subpoenas directed at email service providers for content more than 180 days old.[180] Moreover, documents stored in the cloud[181] are subject to government

---

business." *Id*.

[177] 18 U.S.C. § 2510-22 (1986)

[178] Charles Doyle, Senior Specialist in American Public Law, *Privacy: An Overview of the Electronic Communications Privacy Act*, Cong. Research Service 1 (Oct. 9, 2012), *available at* www.fas.org/sgp/crs/misc/R41733.pdf.

[179] Scott Alford, *Top Ten Reasons to Reform Digital Privacy Rights*, FREEDOM WORKS (Aug. 5, 2013), *available at* http://m.freedomworks.org/blog/backtoliberty/top-ten-reasons-to-reform-digital-privacy-rights. Under the ECPA, a "single email or document is subject to separate legal standards as it's written, sent, and opened." *Id.*

[180] 18 U.S.C § 2703(a); *see* Bridget M. Rohde & Sara J. Crasson, *Government Access to Email and Data Storage Online*, 249 N.Y L.J. 19 (Jan. 29, 2013), *available at* www.mintz.com/DesktopModules/Bring2mind/.../Download.aspx? An individual may challenge a subpoena in court, "but challenges to subpoenas, particularly grand jury subpoenas are rarely successful." *Id.*

[181] Eric Griffith, *What is Cloud Computing?* PCMAG (Mar. 13, 2013), *available* http://www.pcmag.com/article2/0,2817,2372163,00.asp. The author explains cloud computing as follows:

> Cloud computing involves storing and accessing data and programs over the Internet instead of [using the] computer's hard drive. The cloud is just a metaphor for the internet. … [w]ith an online connection, cloud computing can be done anywhere, any time."

Id. *See* Alford, *supra* note 179. To illustrate the danger of the cloud on privacy rights, the author explains the following:

> Under modern technology, the ECPA rules weaken protection on emails and documents. For example, if the document is stored on a desktop computer, it is fully protected by the warrant requirement of the Fourth Amendment. However, the ECPA permits the same document to be searched without a warrant if it is stored with service provider—on the cloud.

Id.

examination.[182] The ECPA also introduces a more relaxed requirement for seeking pen register warrants: law enforcement officials must demonstrate "the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[183]

3. PATRIOT ACT and the Arrival of Section 215 and Section 702

FISA and ECPA underwent major cosmetic changes following the aftermath of September 11 after Congress realized that America's homeland security apparatus needed significant upgrades in the area of collecting, processing, and analyzing foreign intelligence.[184] Congress ushered in the PATRIOT ACT of 2001,[185] as a way to marshal U.S. defense capabilities against threats posed overseas. As a result, access to information became more liberal than the standards imposed in FISA and ECPA. Whereas pen register devices under the ECPA had exclusive use for telephone communications, the PATRIOT ACT employed pen registers to track information flowing through cyberspace.[186] One of the significant changes emanating from the PATRIOT ACT was Section 215.[187] Section 215 permits the Director of the FBI to:

---

[182] Rohde & Crasson, *supra* note 180. Courts have validated warrants that grant access "to all contents of an email account and such warrants have been upheld when challenged as being unconstitutionally overbroad. … Because the government appears ex parte before the court when seeking a search warrant, there is no opportunity to challenge a warrant before it is issued." *Id.*

[183] 18 U.S.C. § 3122(b)(2).

[184] *See* Recess Reading: An Occasional Feature of the Judiciary Committee-The USA Patriot Act, S. COMM. ON THE JUDICIARY, *available at* http: //www.judiciary.senate.gov/about/history/PatriotAct.cfm. (last viewed on Feb. 22, 2014).

[185] *See generally,* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107–56, 115 Stat. 271 (2001).

[186] 18 U.S.C. § 3121(b); *see also* 115 Stat. 271 § 216(3)(A).

[187] *See* 50 U.S.C § 1861.

> make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.[188]

The Snowden disclosures of June 2013 revealed the U.S. government collected telephone metadata[189] pursuant to the FBI's

---

[188] *Id.*

[189] Bradbury, *supra* note 156, at 2. Bradbury's interpretation of the metadata acquired is stated as follows:

> The metadata acquired under [the] order consists of the transactional information that phone companies retain in their systems for a period of time in the ordinary course of business for billing purposes and that appears on typical phone bills. It includes only data fields showing which phone numbers called which numbers and the time and duration of the calls. The order does not give the government access to any information about the contents of the calls or any other subscriber information, and it does not enable the government to listen or record any calls.

Id. For an opposing viewpoint on the validity of the metadata collection, *see* Laura K. Donahue, *Bulk Metadata Collection: Statutory and Constitutional Considerations* 49 (forthcoming in HARV. J. L. & PUB. POL'Y (2014)), *available at* http://justsecurity.org/wp-content/uploads/2013/10/Just-Security-Donohue-PDF.pdf. Donahue asserts the government's argument that the Section 215 metadata is appropriately aligned with 50 U.S.C 1861 based on the reality that "all telephone calls in the United States, including those of a wholly local nature, are 'relevant' to foreign intelligence investigations" and are of assistance to the NSA in bridging gaps between disparate terrorist targets is flawed. *Id.* Donahue's argument is explained as follows:

> whereas in relevance implies a "demonstrably close connection between two objects … [and] some sort of actual connection to a particular investigation … almost none of the information obtained by the government under the bulk metadata collection program is demonstrably linked to an authorized investigation. … In other words, most of the information collected does not relate to individuals suspected of any wrongdoing. … [T]he act suggests that tangible things are presumptively relevant where they: pertain to - (i) a foreign power or agent of a foreign power, (ii) the activities of a suspected agent of a foreign power or who is

request for information under Section 215.[190] The U.S. government justified the acquisition based on necessity, claiming that preservation of the data was critical considering the phone companies temporarily hold the information in their normal business operations.[191] Furthermore, the government wanted to synthesize data derived from many different sources into one database as a way to facilitate recognition of calling patterns.[192] The presence of the database, moreover, was regarded as an integral component in "[conducting] focused-link analysis of terrorist phone numbers," which could accelerate the timeframe of the investigation process.[193] In response to claims of inevitable privacy intrusions as a result of the broad "relevance" language in Section 215, officials in the U.S. government have continued to reiterate the paramount importance of combating attacks by foreign belligerents.[194] The U.S. government cited various protections available to effectively challenge a Section 215 request, including:

> the prior approval of the FISA court, (2) the fact that the phone companies may challenge the scope and legality of the order before the court, (3) the court-ordered limitation that queries of the database may only be conducted for individual phone numbers where the government has a reasonable articulable suspicion that the number is

---

> the subject of an authorized investigation or (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of an authorized investigation. … [H]ere it would be impossible to establish that all customer and subscriber records pertain to a foreign power or an agent..

Id. at 50-51.

[190] Bradbury, *supra* note 156, at 2.

[191] *Id.*

[192] *Id.*

[193] *Id*. at 7.

[194] *Id.* at 9. *See also* Dianne Feinstein, *NSA's Watchfulness Protects America,* WALL STREET J. (Oct. 14, 2013), *available at* http://www.feinstein.senate.gov/public/index.cfm/2013/10/the-nsa-s-watchfulness-protects-america-wall-street-journal. The ability to connect the dots through an analysis of phone numbers and length of calls is regarded as a necessary precondition to averting incidences of terrorism. *Id.*

> associated with a particular foreign terrorist organization, (4) the prohibition on using the database for any other purpose and the requirement that it be kept segregated from other data, (5) the restrictions on the number of officials who can approve access to the database and the other oversight and reporting requirements that apply to the program, and (6) the extensive minimization procedures that govern the retention and dissemination of any information about U.S. persons generated from the database.[195]

Despite these assertions from the government, critics have commented otherwise. One being that Section 215 expressly allocates the responsibility of collection to the FBI, not the NSA, and therefore the NSAs actions are adding to an already overloaded collection regime.[196] Moreover, commentators have attributed Section 215 to a growing chasm between the government and American people. The belief is that when the government can control the flow of data, there is an ever present danger that the full

---

[195] Bradbury, *supra* note 156, at 9.

[196] 50 U.S.C § 1861 (a)(1); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD: REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 11 (Jan. 23, 2014), *available at* http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf. [hereinafter PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD]. "The [Privacy and Civil Liberties Oversight Board (PCLOB)] is an independent bipartisan agency within the executive branch established by the Implementing Recommendations of the 9/11 Commission Act of 2007." *Id.* at 2. The role of the PCLOB is stated as follows:

> The Board is comprised of four part-time members and full-time chairman, all appointed by the President and confirmed by the Senate. The Board's authorizing statute gives it two primary responsibilities:
>
> 1) To analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with need to protect privacy and civil liberties; and
>
> 2) To ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.

Id. at 2.

force of the law may act to restrain civil liberties and subject individuals to targeted blackmail and scrutiny.[197] Section 702 of the Foreign Intelligence Surveillance Act[198] "authorizes PRISM to collect without a warrant, the electronic communications of foreign targets reasonably believed to be both non-citizens and outside the United States."[199] As a preliminary step, the Attorney General and the Director of National Intelligence "make and submit to the FISA court written certifications for the purpose of acquiring foreign intelligence information."[200] In order for collection to proceed, the FISC must approve the targeting procedures under which the surveillance occurs and the minimization procedures that govern use of the acquired information.[201] The scope of surveillance covered under Section 702:

> encompasses surveillance of telephone and internet communications and the NSA's internet collection under this authority includes both (1) electronic communications and stored communications acquired directly from internet service providers, and (2) electronic communications acquired at "upstream" points on the internet backbone networks.[202]

If the FISC approves of the petition to target foreign individuals

---

[197] *Id.* at 12. The PCLOB did note that despite the "remote" danger present by such disclosure, "given the historical abuse of personal information by the government during the 20th century, the *risk is more than theoretical*." *Id.* Recent revelations "involving the targeting of groups based on ideology or religion"; specifically the Internal Revenue Service (IRS) singling out the Tea Party raises concerns over the government's rampant misuse of surveillance authority. *Id.* at 160.

[198] 50 U.S.C. § 1881(a); *see* Etzioni, *supra* note 96, at 20;

[199] Bradbury, *supra* note 156, at 10.

[200] NATIONAL SECURITY AGENCY: MISSIONS, AUTHORITIES, OVERSIGHTS, AND PARTNERSHIPS 4 (Aug. 9, 2013), *available at* http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf. [hereinafter NSA MISSIONS]

[201] *Id.*

[202] Bradbury, *supra* note 156, at 10.

overseas, internet service providers are obligated to support the federal government in its collection efforts.[203] This support comes in the form of using personal data, such as e-mail addresses supplied by the NSA to monitor persons of interest overseas who are potential recipients of foreign intelligence information.[204] In its most critical role, Section 702 is used by the NSA to anticipate and defuse terrorist plots globally.[205]

4. HIPAA and the Affordable Care Act

In 1996, Congress made significant efforts to shelter confidential medical information from third parties by passing the Health Insurance Portability and Accountability Act (HIPAA).[206] HIPAA desired a shift toward the digitization of medical records out of concern for physician access.[207] Despite instituting several privacy measures,[208] HIPAA's provisions have been regarded as impractical

---

[203] NSA MISSIONS, *supra* note 200, at 4.

[204] *Id.*

[205] *Id.*

[206] Daniel J. Solove, *HIPAA Turns 10: Analyzing the Past, Present, and Future Impact*, 84 J. AHIMA 22, 24 (2013), *available at* http://ssrn.com/abstract =2245022. There was no regulation that ruled over all the different individuals and entities that dealt with health data. For that reason, HIPAA's main objective was to "create a set of uniform electronic healthcare transaction codes." *Id.*

[207] McFarland, *supra* note 153. Even though records in electronic form provide support for physicians located in distant locations away from the patient's hometown and promote more efficient billing procedures, the luxury of accessibility is tempered by the fact having information instantaneously makes it more visible to unwanted third parties. *Id.*

[208] *Guide to Privacy and Security of Health Information*, DEP'T OF HEALTH AND HUMAN SERVICES: OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., *available at* http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide-chapter-4.pdf (last visited Oct. 25, 2013). The HIPAA Privacy Rule provides "individuals with privacy rights and [helps] individuals understand and control how to their health information is used." *Id.* at 28. One of the features of the Privacy Rule is the "minimum necessary rule." *Id.* Under the rule, health care providers must use the least possible protected information to carry out an activity. *Id.* at 29.

and burdensome.[209] While HIPAA regulates transmissions of data in professional settings, it does not lay out a procedure to prevent unauthorized communications in more informal settings.[210] Recent requirements under HIPAA have addressed some of these concerns;[211] requiring entities to implement several modifications to enhance protection of medical information as part of the Affordable Care Act (ACA).[212] However, some have argued that the onset of the ACA may jeopardize HIPAA's progressive privacy rules.[213]

---

[209] Ericka Adler, *Oops You're Violating HIPAA and Didn't Even Know it,* PHYSICIANS PRACTICE (Aug. 31, 2011), *available at* http://www.physicians practice.com/blog/oops-you%E2%80%99re-violating-hipaa-and didn%E2%80% 99t-even-know-it. HIPAA does not provide a clear enforcement mechanism for conversations made at doctor offices that contain protected health information under HIPAA that would be used for identity theft. *Id.* For example, receptionists have posted messages on Facebook regarding the patient's medical issue. *Id.* This information is then made privy to Facebook friends and common acquaintances. *Id.* Some doctor offices recommend "computer access should be password protected and there should be strict rules regarding the use of social media," but this has not translated into a federal rule. *Id.*

[210] McFarland, *supra* note 153.

[211] *New HIPAA Privacy Law, Security Rules take Effect on September 23,* AM. ACAD. OF PEDIATRICS (Jul. 11, 2013), http://aapnews.aappublications.org/ content/early/2013/07/11/aapnews.20130711-1. The Academy enumerated the procedures required under the new mandate which "provide individuals new rights to their health information, enhance patient privacy protections and strengthen the government's ability to enforce the law …expand an individual's right to receive electronic copies of his or her health information; …prohibits most health plans from using or disclosing genetic information for underwriting purposes." *Id.*

[212] *See The Affordable Care Act: A Brief Summary,* NAT'L CONFERENCE OF STATE LEGISLATURES (Mar. 2011), *available at* http://www.ncsl.org/ portals/1/documents/health/hraca.pdf. Some of the key federal provisions include "expand[ing] access to insurance, increase[ing] consumer protections, emphasiz[ing] prevention and wellness, improve[ing] quality and system performance, expand[ing] the health workforce, and curb[ing] rising health care costs." *Id.* With regard to "quality and system performance, the ACA uses data collection and reporting mechanisms to address health disparities among populations based on ethnicity, geographic location, gender, disability status, and language." *Id.*

[213] *States Raise Concerns over Health Law Navigators,* THE HILL (Aug. 17, 2013), *available at* http://thehill.com/blogs/healthwatch/health-reform-implementation/317513-state-attorneys-general-raise-privacy-concerns-over-obamacare-navigators. Navigators assist in the registration process by helping

Reviving the 1960s proposal for a National Data Center, the Affordable Care Act has established the "Federal Data Services Hub," a segment of the health insurance exchanges,[214] which has focused on interlinking agency access to personal information of individuals seeking health care coverage.[215]

---

interested parties "navigate through the paperwork of the new healthcare system." *Id.* Due to time constraints with the implementation of the ACA, the Department of Health and Human Services (HHS) cut back on "background checks and eliminating a fingerprinting requirement [for the navigators], which could make it easier for a person's private information to fall into the wrong hands." *Id.* There are still unanswered questions as to the manner of liability if personal information is stolen by a navigator as well as fraud prevention education for the navigators. *Id.*

[214] *Health Insurance Exchanges: A Strategic Perspective*, DELOITTE (2011), *available at* http://amcp.org/WorkArea/DownloadAsset.aspx?id=10594. "Section 1311 of the ACA requires each state to establish an "exchange" or marketplace to provide health plans." *Id.* at 1. Some of the main functions of the exchanges are to "certify or decertify qualified health plans…and establish the "Navigator" program." *Id.* at 2.

[215] Mike Rogers, Chairman of the House Intel. Comm., *Obamacare Data Hub Looms as a Privacy Threat: Column*, USA TODAY (Oct. 10, 2013), *available at* http://www.usatoday.com/story/opinion/2013/10/10/obamacare-exchange-federal-data-hub-column/2958681/. The hub connects "seven different agencies and establish new access points to sensitive personal information of the American public." *Id. See* Stacy Cowley, *How Obamacare's Privacy Nightmare Database Really Works*, CNN MONEY (Jul. 24, 2013), *available at* http://money.cnn.com/2013/07/23/technology/security/obamacare-privacy/. The data hub acts as a "middleman reaching out to seven different federal agencies to view information about those seeking coverage." *Id.* The Department of Health and Human Services provided a list of federal data sources its hub will be gathering:

> The Internal Revenue Service will collect information on adjusted gross income, family size, filing status (married or single), and calculation of tax credits to assess eligibility for tax credits. The Social Security Administration will validate social security numbers, social security benefit payments, and incarceration status. The Department of Homeland Security (DHS) will verify immigration status. The Department of Defense, Department of Veterans Affairs, and Office of Personnel Management will check to see whether the applicant is "enrolled in health care programs run by these departments."

Id.

5. A Detour into Supreme Court Privacy Jurisprudence

The 14th Amendment Due Process Clause bars any state from depriving "any person of life, liberty, or property, without due process of law."[216] Through judicial interpretation, this clause spawned the creation of a "zone of privacy," which regards certain rights as "fundamental" or "implicit in the concept of ordered liberty,"[217] and "deeply rooted in this nation's history and tradition."[218] The Supreme Court has extended this fictional zone to cover the following: the right to purchase contraceptives;[219] the right to not have undue burdens placed on the decision to have an abortion;[220] the right to maintain intimate relations;[221] the right to

---

[216] U.S. CONST. amend. XIV, § 1.

[217] Helen L. Gilbert, *Minors' Constitutional Right to Information Privacy,* 74 U. CHI. L. REV. 1375, 1377 n. 16 (2007) (citing to *Roe v. Wade*, 410 U.S 113, 152–53 (1973), quoting *Palko v. Connecticut*, 302 US 319, 325 (1937)).

> The Supreme Court first announced this right to privacy in *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965), rooted in the "penumbras" of the First, Third, Fourth, Fifth, and Ninth Amendments. In *Roe v Wade*, the Court grounded the right to privacy in the "Fourteenth Amendment's concept of personal liberty." 410 U.S. at 153.

Gilbert, at n. 16.

[218] *Id.* at 1377 n. 17. This concept was referred to in *Moore v. City of East Cleveland*, 431 U.S. 494, 503 (1977).

[219] Griswold, 381 U.S. 479, at 484-486 (1965). Following *Griswold*, the Supreme Court heard its companion case, *Eisenstadt v. Baird*, 405 U.S. 438 (1972). In *Eisenstadt*, the Court extended the right to use contraceptives to married couples finding that it is the "right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child." *Id.* at 453.

[220] Roe, 410 U.S. at 154. The Court noted the fundamental right to privacy is expansive enough to encompass a woman's decision whether or not to terminate her pregnancy but "this right is not unqualified and must be considered against important state interests." *Id.* Subsequently, the Court heard *Planned Parenthood of Se. Pa. v. Casey*, 505 U.S. 833 (1992), which reaffirmed the fundamental nature of the right to abortion. The *Casey* Court espoused the importance of the right when it stated that "at the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life." *Id.* at 851.

[221] *See* Lawrence v. Texas, 539 U.S. 558, 578 (2003) (striking down a Texas law prohibiting a couple from engaging in a homosexual lifestyle).

dictate family upbringing[222] and education of children;[223] and the right to marry and procreate.[224]

The Supreme Court has wrestled with how information privacy fits within the zone's boundaries.[225] In 1977, the Supreme Court addressed information privacy in *Whalen v. Roe*.[226] In *Whalen*, a New York Statute authorized a centralized system to process and store prescription drug information.[227] The *Whalen* majority, applying the police powers of the Tenth Amendment, held the New York law fell within the state's police power to collect medical information in order to stifle the circulation of illegal drugs.[228] The Supreme Court delineated the right to privacy into two distinct subparts: (1) "the individual['s] interest in avoiding disclosure of personal matters"[229] and (2) "the interest and independence in making certain kinds of important decisions."[230] The court found little evidence in the record supporting the idea of poor oversight or

---

[222] *See* Pierce v. Society of Sisters, 268 U.S. 510, 532-535 (1925) (striking down a law mandating parents to transfer their children from private Catholic school to public schools).

[223] *See* Meyer v. Nebraska, 262 U.S. 390, 401 (1923) (striking down a Nebraska law that forbade the teaching of a foreign language in the classroom, which infringed on students' rights to learn and the parents' right to determine the education of their children).

[224] *See* Skinner v. Oklahoma, 316 U.S. 535 (1942). The Supreme Court struck down an Oklahoma law sterilizing individuals convicted of felonies of "moral turpitude." *Id.* at 537. In crafting its holding, the Court chastised the Oklahoma law as a direct affront to the very survival of the human race "marriage and procreation," which warranted the application of strict scrutiny: requiring the government to show a compelling interest for the law. *Id.* at 541.

[225] Fred H. Cate & Beth E. Cate, *The Supreme Court and Information Privacy*, INT'L DATA PRIVACY L. 1 (2012), *available at* http://idpl.oxford journals.org/content/early/2012/09/26/idpl.ips024.full.pdf+html.

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

[227] *Id.* at 591.

[228] *Id.* at 598.

[229] *Id.* at 599. *See Safeguarding Privacy in the Fight Against Terrorism*: *The Report of the Technology and Advisory Committee*, DEP'T OF DEF. TECH. & PRIVACY ADVISORY COMM. 25 (Mar. 2004). Even though the Court recognized an interest in non-disclosure, the "Court did not apply strict scrutiny—which it typically reserves for cases involving fundamental interests." *Id.*

[230] Whalen, 429 U.S. at 599-600.

improper administration over patient information.[231] Since the statute's protections did not adversely affect existing medical care,[232] Part IV of the *Whalen* opinion, despite acknowledging the existence of a threat to privacy through the collection of sensitive data,[233] refused to decide "any question which might be presented by the unwarranted disclosure."[234] The court's reasoning hinged on the fact that it was a mere possibility that such events could occur.[235] The Court made clear that the disclosure of information required by the New York statute was not any different from the "other unpleasant invasions of privacy" linked with the health care industry.[236]

Following *Whalen,* the Supreme Court was again presented with an opportunity to draw a bright-line rule regarding information privacy. In *Nixon v. Administrator of General Services,*[237] President Nixon brought suit disputing the constitutionality of the Presidential Recordings and Materials Preservation Act.[238] The Act authorized the Administrator of General Services to take possession of all "papers, documents, memorandums, transcripts, and other objects and materials which constitute the Presidential historical materials."[239] Furthermore, the Act permitted screening for archival purposes and placed limitations on future public access to such records. [240] In assessing the degree of privacy accorded to President Nixon's documents, the *Nixon* court found a privacy interest in the intimate correspondence between the President, his family members, physician, and minister, but not in every communication made within the scope of his official duties.[241] *Whalen* and *Nixon* illustrated that the state's preference for information outweighed

---

[231] *Id.* at 601.

[232] *Id.* at 605.

[233] *Id.*

[234] *Id.*

[235] Christina Moniodis, *Moving from NASA to Nixon: Privacy's Second Strand—A Right to Informational Privacy,* 15 YALE J.L & TECH. 139, 145 (2012).

[236] *See* Whalen, 429 U.S. at 602.

[237] *See* Nixon v. Adm'r of Gen. Serv., 433 U.S. 425 (1977).

[238] *Id.* at 430.

[239] *Id.* at 434.

[240] *Id.* at 436.

[241] *Id.* at 459.

individual concerns over disclosure.[242] Decades later, the Supreme Court, in 2011, heard *NASA v. Nelson*.[243] *Nelson* examined the constitutionality of background checks for federal contractors.[244] In examining the procedures surrounding the background checks, the Court found that "reasonable employment inquiries," including those related to drug consumption were proper to determine whether an applicant was fit for civil service.[245] Given the magnitude of the work performed and its national consequences, the Court harped on the "Government's interest in managing its internal operations."[246] The *NASA* court, reflecting previous sentiments regarding the state of information privacy, did not conclude the existence of privacy infringement because the likelihood that the answers to the questionnaires would be released was attenuated at best due to preventative measures already in place.[247]

6. Standing Issues

With unclear parameters for privacy enforcement, individuals seeking recourse from the judicial system for damages have faced

---

[242] Moniodis, *supra* note 235, at 142. The Whalen and Nixon decisions "ruled in favor of the state," which prevented a future right to non-disclosure of information. *Id.*

[243] *See* NASA v. Nelson, 131 U.S. 746 (2011).

[244] *Id.* at 751. The respondents "challenged a section in the questionnaire asking employees about treatment or counseling for recent illegal-drug abuse." *Id.*

[245] *Id.* at 759.

[246] *Id.* at 760. In this instance, the government does not have the burden "when it requests job-related personal information in an employment background check…to demonstrate that its questions are necessary or the least restrictive means of furthering its interests." *Id.* The government argued that if it framed its questions "in more permissive terms, [it] would [receive] a lower response rate, and the question's effectiveness in identifying illegal drug users who are suitable for employment would be "materially reduced." *Id.* The Court also remarked that the "pervasiveness [of such questions] in the private and public sectors" indicate this method of questioning is an effective way of "identifying capable employees who will faithfully conduct the government's business." *Id.* at 761. In NASA, the form in question was distributed "over 1.8 million times annually." *Id.*

[247] *Id.* at 763.

standing issues.[248] Plaintiffs argue they are at a particular disadvantage in "data breach cases,"[249] and cannot adequately seek redress for their injuries because (1) in many instances there is difficulty showing a link[250] between the actual data breach and the misappropriation of private data;[251] (2) there is confusion on which

---

[248] Kim Phan, *Assessing Risk: Data Breach Litigation in U.S. Courts*, INT'L ASS. OF PRIVACY PROF'L (Nov. 1, 2012), *available at* https://www.privacyassociation.org/publications/2012_11_01_assessing_risk_data_breach_litigation_in_u.s._courts. Under Article III of the U.S. Constitution, Plaintiffs must have standing to proceed in a lawsuit. *Id.* A component of having standing is a showing of an "injury-in-fact," which "requires a concrete and particular harm that is actual and imminent." *Id*. *See U.S. Courts Continue to Grapple with Article III Standing Issues in Internet Privacy Cases*, MAYER BROWN 1 (2011), *available at* http://www.mayerbrown.com/files/Publication/1e129ba7-a74f-4582-b422-6deecf4c6b52/Presentation/PublicationAttachment/1761bec4-6efd-459b-93d7-3c7c327d303d/11656.pdf [hereinafter *Internet Privacy Standing*]. The injury must be "fairly traceable" to the violation alleged. *Id.* Moreover, there must be a form of redress available to the Plaintiff. *Id.*

[249] DEPARTMENT OF JUSTICE: DOJ INSTRUCTION ON INCIDENT RESPONSE PROCEDURES FOR DATA BREACHES 4 (Aug. 6, 2013). Breach is defined as including:

> the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to information, whether physical or electronic. It includes both intrusions [inside and outside] the organization.

Id. See Timothy Madden, *Data Breach Class Action Litigation-A Tough Road for Plaintiffs*, B. BAR J. (Fall, 2011), *available at* http://www.bostonbar.org/pub/bbj/bbj_online/bbj1112/fall2011/LegalAnalysis2.pdf. "Data breaches generally take one of two forms: the accidental loss of electronic records containing personally identifiable information (lost laptop, accidental e-mailing of records) or intentional and unauthorized intrusion into an organization's computer … and subsequent theft of information … (hacking)." *Id*. at 28.

[250] *See Internet Privacy Standing*, *supra* note 248, at 1.

[251] DEPARTMENT OF JUSTICE, *supra* note 40, at 4. Personal information or Personally Identifiable Information (PII) is:

> any information about an individual maintained by an agency including: (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, and mother's maiden name, (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Information that standing alone is not

specific state and federal law claims can be used to state a particular claim for relief;[252] and (3) the novelty[253] of data breach cases complicates the pleading process for such claims.[254] Given the range of harms[255] that may result from a data breach, consumer plaintiffs

---

> generally considered personally identifiable, because many people share the same trait include: (1) first or last name, if common, (2) country, state, city, or zip code of residence, (3) age, especially if non-specific (such as age in years, without a birthdate), (4) gender or race, (5) workplace or school, and (6) grades, salary, or job description.

Id.

[252] Madden, *supra* note 249, at 29. Some common causes of actions applicable in a data breach case include negligence, breach of contract, breach of fiduciary duty, negligent misrepresentation, and violation of consumer protection laws. *Id.* Plaintiffs have resorted to state-based data protection laws but this course of action has routinely failed. *Id.*

[253] *See Internet Privacy Standing*, *supra* note 248, at 3. Standing will continue to pose a problem for courts with respect to data breach claims unless more cases are heard by upper-level courts whose rulings will give "authoritative guidance" on the issue. *Id.*

[254] *Id.* The authors highlight *Spokeo* as an important case in illustrating the complexity in pleading such cases. In *Spokeo*:

> Plaintiff sued Defendant under violations of the Fair Credit Reporting Act (FCRA) alleging that Defendant inaccurately posted wrong information about him, acted as a consumer reporting agency. Plaintiff argued in his initial complaint that as a consumer agency, Defendant was required to take necessary precautions or make certain disclosures under the FCRA. In his initial complaint, Plaintiff, who was unemployed, alleged that the inaccuracies posted on the site would impinge on future employment prospects. Defendant made a request for dismissal on the grounds that the injury alleged was merely "hypothetical" and not "actual or imminent." The trial court agreed with Defendant. When Plaintiff filed an amended complaint adding on claims that the posting of inaccurate information caused emotional distress, the trial court found the posting of information to be "fairly traceable" to the FCRA violations enumerated by the Plaintiff. On appeal, the district court found that Plaintiff actually lacked standing and dismissed the case ruling that the employment prospects were too speculative, making the point that Plaintiff failed to allege facts connected to the alleged FCRA violations.

Id.

[255] M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1142 (2011). To illustrate the complexity of the harms that could potentially be brought into litigation, Calo lays out "two categories of privacy harms: subjective harms and objective harms." *Id.* On one hand, subjective harms are internal and "flow

argue continued stalemate within the federal circuit courts[256] in the development of an approach[257] to quantify the harm resulting from a data breach is crucial given the consequences of dismissal for the Plaintiff.[258] Individuals who have lost confidential, sensitive, personal information are more inclined to "feel violated and harmed

---

from the perception of unwanted observation." *Id.* Subjective harms "can be acute or ongoing, and can accrue to one individual or to many," and can vary "in severity from mild discomfort at the presence of a security camera to mental pain and distress far greater than could be inflicted by mere bodily injury… actual observation need not occur to cause harm; perception of observation can be enough." *Id.* On the other hand, objective harms "involves the forced or unanticipated use of information about a person against that person," such as when personal information is used to justify adverse action against that person ("government leverages data mining or sensitive information to block a citizen from air travel," creating gossip, or identity theft). *Id.* at 1143.

[256] *See* Anderson v. Hannaford Brothers Co., 659 F.3d 151, 162-167 (1st Cir. 2011) (holding Plaintiffs' foreseeable mitigation costs including credit monitoring constitute a cognizable harm as it is reasonable that a consumer would take the necessary steps to mitigate damages in light of fraudulent activity); *see* F.T.C v. Neovi, Inc., 604 F.3d 1150, 1157 (9th Cir. 2010) (finding "concrete and quantifiable" injury when consumers "were injured by a practice they did not bargain" for); Reilly v. Ceridian, 664 F.3d 38, 42 (3rd Cir. 2011) (denying a claim of data breach in the absence of an injury which did not result in "misuse of [personal] information").

[257] *See* Mark McCarthy, Professor of Information Privacy and Technology Policy at Georgetown University, *New Directions in Privacy: Disclosure, Unfairness, and Externalities* (Jun. 2010), *available at* http://www18.georgetown.edu/data/people/maccartm/publication-51099.pdf. The author supports the application of an approach called the unfairness method, which is adopted by the Federal Trade Commission to current privacy regulation, particularly to supplement the current informed consent model. *Id.* at 5. Under the FTC Act, an "information practice would be unfair when it imposes substantial injury on consumers that is not easily avoidable and which does not have compensating benefits." *Id.* Whereas the informed consent model presupposes that consumers follow the "myriad ways in which information leaks," the unfairness model does not impose the expectation on the consumer that he must "master the ways in which information can be collected and used. *Id.* at 60. McCarthy advances the idea that there should be a "substantive evaluation" of the use of the data instead of just curbing collection. *Id.*

[258] Madden, *supra* note 249, at 29. If the Plaintiff cannot demonstrate that information is compromised, the Plaintiff will have to relegate his damages, basing his relief on "aggravation and emotional distress" and will have to expend extra resources safeguarding against the potential for future fraud or identity theft. *Id.*

by the experience."[259]In terms of government surveillance, standing issues present similar difficulty for plaintiffs to prove that the algorithmic process used by the NSA—to distinguish between data that may reveal the existence of a terrorist group versus harmless data with no value—deliberately compromises the confidentiality of their data. A compelling example of this challenge came in *Clapper v. Amnesty Int'l.*[260] The plaintiff, Amnesty International brought suit claiming their line of work, which involved communicating with individuals overseas was jeopardized by Section 702's targeted surveillance on foreigners connected with terrorist organizations.[261] Amnesty argued there was an "objectively reasonable likelihood that their communications would be acquired . . . at some point in the future."[262] In taking precautionary measures to avoid interception, Amnesty claimed it had to revert to alternative means of communications, other than telephone or email, which required additional travel expenses to meet with their colleagues.[263]

The Supreme Court concluded that Amnesty's claim rested on pure speculation, requiring of chain of inferences to be made that the government would single out the communications at issue, that the FISC would make the finding that the interceptions satisfied the Fourth Amendment, and that the government would be able to intercept the communications of which the plaintiff's colleagues were party to those communications.[264] Because of the inherent secrecy underlying the data collection process, the government, not Amnesty International, would have intimate knowledge of the methods behind the selection of suspected communications.[265] Thus, the majority held that Amnesty did not meet its burden in showing that government data collection was "certainly impending" or that such collection affected Amnesty intimately and not incidentally.[266]

---

[259] *Id.* at 33.
[260] Clapper v. Amnesty Int'l, 133 S.Ct. 1138 (2013).
[261] *Id.* at 1142.
[262] *Id.* at 1143.
[263] *Id.* at 1146.
[264] *Id.* at 1148.
[265] *Id.* at 1149-50.
[266] *Id.* at 1150-51.

B. India

1. Indian Constitutional Law and Issues of Privacy and Surveillance

The Indian Constitution of 1950[267] does not explicitly assert a general right to privacy[268] or alternatively recognize privacy as a fundamental right.[269] The Indian privacy right is implicit within the Indian Constitution by interpretation through the Indian Supreme Court "as a component of two fundamental rights: the right to freedom under Article 19 and the right to life and personal liberty under Article 21."[270] Article 19 and 21, however, give deference to government policies and are vulnerable to restriction:

> Article 19(a)(1) stipulates that all citizens shall have the right to freedom of speech and expression. . .qualified by Article 19(2) which states that this will not affect the operation of any existing law or prevent the State from making any law, insofar as such law imposes reasonable restrictions on the exercise of the right. . .in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency, or morality, or in relation to contempt of court, defamation, or incitement to an offense. . . Article 21 states that no person shall be deprived of his life or personal liberty except according to procedure established

---

[267] *Constitution of India,* EMB. OF INDIA, BEIJING, *available at* http://www.indianembassy.org.cn/ConstitutionofIndia.aspx (last visited Oct. 27, 2013). The Indian Constitution was enacted on January 26, 1950.

[268] Prashant Iyengar, *Privacy in India-Country Report-October 2011*, CTR. INTERNET &SOC. 5 (Oct. 30, 2011), *available at* http://cis-india.org/internet-governance/country-report.pdf. [hereinafter *Privacy in India 2011*]

[269] *Constitution of India*, *supra* note 267. The six categories of fundamental rights in the India Constitution are "right to equality before the law, right to freedom of speech and expression, right against exploitation, right to freedom of conscience and free profession, right to conserve their culture, language, or script, and right to constitutional remedies for enforcement of Fundamental Rights." *Id.*

[270] *Privacy in India 2011, supra* note 268, at 5.

by law.[271]

In *Kharak Singh v. State of UP,*[272] the Indian Supreme Court assessed the state of Uttar Pradesh's surveillance procedures with respect to individuals charged with crimes but later released.[273] Uttar Pradesh permitted its officers to conduct surveillance by following and reporting the individual's movements and making sporadic visitations to his residence.[274] The claims brought forth concerned the invasion of the petitioner's personal liberty under Article 21.[275] The Court construed Article 21 as protecting the dignity of the individual and construed personal liberty to the person and not to property including his house.[276] However, the Court held "the right of privacy is not a guaranteed right under [the Indian] Constitution, and therefore the attempt to ascertain the movements of an individual which is merely a manner in which privacy is invaded is not an infringement of a fundamental right."[277]The Indian Supreme Court extended the notion of individual dignity to material transferred to a

---

[271] *Id.* While the government is given a degree of latitude in restricting the exercise of the right, the author mentions the Indian Supreme Court case of Maneka Gandhi v. Union of India (1978) as an example of a check on that power. *Id.* at 6. In Maneka, "any procedure which deals with the modalities of regulating, restricting or even rejecting a fundamental right falling with Article 21 has to be fair, not foolish, carefully designed to effectuate, not to subvert, the substantive right itself." *Id.* at 6. The procedure must "rule out anything arbitrary, freakish, or bizarre." *Id.*

[272] Kharak Singh v. State of U.P. & Others, A.I.R. 1963 S.C. 1295.

[273] *Id.* at 332.

[274] *Id.*

[275] *Id.*

[276] *Id.* at 333.

[277] *Id.* The court stated that "the secret picketing of the house [merely watching and keeping record] of suspects could not in any material or palpable form affect the right on the part of the suspect to move freely or deprive of him of his Personal liberty … the makers did not intend to protect personal sensitiveness." *Id.* The holding in Kharak is a far stretch from American jurisprudence, whose umbrella stretches over all areas to which a person has a reasonable expectation of privacy [persons and property]. The literal view of the Constitution adopted by India has extraordinary consequences for the mass surveillance trends discussed herein which are authorized absent legislative authorization.

third party in *District Registrar and Collector v. Canara Bank*.[278] In *Canara Bank,* the Court reiterated the concept that privacy "deals with persons and not places and as such, documents and copies residing at the bank must remain confidential in relation to the person even if they are no longer at the customer's house and have been voluntarily sent to a bank."[279] In essence, the nature of the documents is permanent despite the loss of control even if the loss occurs voluntarily.[280]

Furthermore, in *Malak Singh v. State of Punjab & Haryana*,[281] the Indian Supreme court developed a benchmark to assess the basis for lawful surveillance. In *Haryana*, two individuals challenged a surveillance order on the grounds that police had no reasonable belief to label them as criminals and that their presence in the surveillance register was due to their political associations.[282] The Punjab police claimed: (1) the appellants or the public for that matter could not have had access to the register given its character as a confidential document and (2) the type of activity warranting an entry in the surveillance register is "so utterly administrative and non-judicial" that it does not invoke the doctrine of "*audi alteram partem*."[283] The Indian Supreme Court affirmed that surveillance practices are valid if they do not threaten an individual dignity, are not unlawfully invasive and are inconspicuous in nature.[284] Additionally, the Court mandated that the officer, in issuing his surveillance order, must "entertain reasonable belief" that the targeted individuals are "habitual offenders or receivers of stolen

---

[278] District Registrar and Collector v. Canara Bank A.I.R 2005 S.C. 186

[279] *Id.* at 19. As stated in the opinion, the reasoning of the *Canara* court runs counter to the commentary provided in *Smith v. Maryland* and its companion case *United States v. Miller*, which held that an individual relinquishes his right to privacy over information when he voluntarily conveys it to a third party.

[280] *Surveillance and Privacy in India-VII: Summary*, INDIAN CONST. L. & PHIL. (Dec. 23, 2013, 2:27 AM), *available at* http://indconlawphil.wordpress.com/tag/surveillance-2/.

[281] Malak Singh v. State of Punjab & Haryana, A.I.R 1981 S.C. 760.

[282] *Id.* at 313.

[283] *Id.* at 318.

[284] *Id.* at 318-19.

property."[285]

2. Statutory Basis

With respect to data collection and interception of messages, the Telegraph Act of 1885 mirrors the qualified constitutional right to privacy. Section 5(2) of the Telegraph Act grants the Indian government the authority to intercept any messages from any person or class of persons:

> a) on the occurrence of any public emergency, or in the interest of public safety, and
> b) if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offense.[286]

This trend toward giving latitude to government endeavors continued when India became an active participant in cyberspace with the

---

[285] *Id.* at 319.

[286] THE INDIAN TELEGRAPH ACT OF 1885, *available at* http://www.ijlt.in/pdffiles/Indian-Telegraph-Act-1885.pdf (last viewed Feb. 21, 2014). *See Surveillance and Privacy in India*, *supra* note 280. This commentator suggests that Section 5(2) may not be relevant to the current crisis of bulk surveillance:

> First, the Indian Telegraph Act is an 1885 legislation, drafted at a time when bulk surveillance was unimaginable and aimed at addressing a very different problem—interception of *individual* telegraphic messages for specific short-term purposes. Secondly, the term "persons or class of persons" is clearly indicative of *identifiable* individuals (or class of individuals), and is not meant to include the citizenry as a whole…Thirdly, the concept of *public safety or public emergency* cannot be secretive, but must be evident to the reasonable person…Therefore, the Indian Supreme Court's view that targeted surveillance does not need judicial review may not apply for bulk surveillance.

Id.

passage of the New Internet Policy (NIP).[287] During this period, discussion shifted toward the creation of a comprehensive law to address globalization and the growth of e-commerce.[288] By 2000, the IT Act was passed by the Indian legislature.[289] The IT Act acted as a platform to move India away from archaic communication practices[290] and toward greater competence in electronic exchanges.[291] The framework of the IT Act was regarded as unconventional.[292] Even though the IT Act made headway in curbing

---

[287] Nitin Desai, *India's Cybersecurity Challenges,* INST. FOR DEF. STUD. AND ANALYSES (Mar. 2012). NIP ushered in the creation of multiple Internet Service Providers (ISP) seeing the "internet base grow from 1.4 million in 1999 to over 15 million in 2003." *Id.* at 19. *See India Telecom 2000: India Internet Policy and Markets,* INFO. GATEKEEPERS, INC. 37 (1999). The task force involved in carrying out the plan "identified internet proliferation as a key measure in making India an IT superpower." *Id.* at 37.

[288] *See Cyber Laws in India,* INDIAN INST. OF BANKING AND FIN. 2, *available at* http://www.iibf.org.in/docuuments/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf. [hereinafter *Cyber Laws in India*].

[289] *See* Udapudi, *supra* note 14, at 182. Increased technological transactions and India's entrance into cyberspace required the Indian legislature to develop laws that would regulate technology in India. *Id.*

[290] *See Cyber Laws in India, supra* note 288, at 2. A large proportion of international transactions up until the mid -1990s were "done through documents being transmitted through post and by telex only." *Id.* "Evidence and records were predominantly paper evidences and paper records or other forms of hard-copies only." *Id.*

[291] *See* Udapudi, *supra* note 14, at 183. The legislative intent of the IT Act indicated India's departure from previous practices:

> An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

Id.

[292] *See Cyber Laws in India, supra* note 288, at 2. Due to the unprecedented nature of the IT Act, divisions were created among those who viewed the IT Act as "too draconian and others stating it was too lenient and diluted." *Id.* The product of uncertainty created by the split drew more support for earlier laws, which led to the

various computer-related crimes by individuals,[293] particularly unauthorized access,[294] the Act did not address issues of personal privacy protection, including identity theft.[295]

Subsequent national security threats[296] and the skyrocketing development of India's high-tech sector[297] refocused the IT Act on information security practices adopted by third-parties and corporations.[298] The result was an amended version of the IT Act,

---

application of those laws in "technology-based cases." *Id.*

[293] Sanjey Pandey, *Curbing Cyber-Crime: A Critique of the Information Technology Act of 2000 and IT Act Amendment 2008*, *available at* http://www.softcell.com/pdf/IT-Act-Paper.pdf (last visited Nov. 7, 2013). These computer-related crimes included introducing a "virus … causing damage and manipulation [to] computer accounts, acts of hacking leading to wrongful … damage, tampering, destroying and concealing computer code, and acts related to publishing, transmission, or causing publication of obscene/lascivious in nature." *Id. See* Karen M. Sanzaro & Christyne Ferris, *India's New Information Technology Law Impacts Outsourcing Transactions*, STATE BAR OF GA. (Jun. 6, 2009), *available at* http://technologybar.org/2009/06/indias-new-information-technology-law-impacts-outsourcing-transactions/. The IT Act mainly focused on individual-induced harm and not on "systematic data protection" prior to being amended. *Id.*

[294] Pandey, *supra* note 293. The initial IT Act in 2000 addressed "unauthorized access in section 43."

[295] *Id.* The IT Act did "not talk about maintaining [the] integrity of customer transactions" whereas a comparable British law enacted in 1998 stipulated that "banks or any person holding sensitive information may be held liable for damages if it fails to maintain adequate security protection with respect [to] data." *Id. See* Sanzaro & Ferris, *supra* note 293. "The [initial] IT Act punished unauthorized extraction of or damage to data, but it did not explicitly targeted personal data." *Id.*

[296] *See Cyber Laws in India*, *supra* note 288, at 3. The Mumbai bombings of 2008 forced the Indian government to take swift measures to safeguard sensitive data. *Id.* at 3. *See* Sanzaro, *supra* note 293. "Increases in cybercrimes generally, coupled with the terrorist in attack in Mumbai, [which was carried out] through coordinated technology efforts, [likely contributed to the] passage of the ITAA." *Id.*

[297] *Id.*

[298] *See* Karen Lawrence Oqvist, *New Privacy Legislation for India*, VIRTUAL SHADOWS (Jun. 14, 2009), *available at* http://virtualshadows.wordpress.com/2009/06/14/new-privacy-legislation-for-india/. Section 43(a) of the ITAA is "designed to hold companies [doing business in India or with Indian entities] accountable for the protection of personal data."

> Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns,

known as the Information Technology Act of 2008 (ITAA).[299] Under ITAA, the Indian legislature expanded the range of non-compliant[300] acts and maximized penalties for violations of privacy.[301] The ITAA's provisions for "reasonable security practices and procedures"[302] recognized the concept of sensitive personal data, but gave the Indian Government room to determine the level of sensitivity on a case by case basis.[303]The ITAA also presented new challenges in the realm of individual privacy and free expression in the use of social media and other electronic platforms, particularly Section 66A, Section 69, 69B and 70B. Section 66A states the following:

> controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Id; see Graham Greenleaf, Promises and Illusions of Data Protection in Indian Law, 1 INT'L DATA PRIVACY L. 47, 51 (2011). A body corporate "means any company and include[ing] a firm, sole proprietorship, or other association of individuals engaged in commercial and professional activities." *Id. See* Sanzaro & Ferris, *supra* note 293. The amendment acknowledged that "corporations and intermediaries" and not just individuals, "bear some [of the] responsibility in ensuring data in their possession is secure." *Id.*

[299] THE INFORMATION TECHNOLOGY ACT OF 2008, *available at* http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf (last visited Feb. 20, 2014). [hereinafter IT ACT 2008]

[300] *Id.* The act of "destroy[ing], delet[ing], or alter[ing]" information or decreasing the value or utility of the information, was added to the amended IT Act.

[301] *Id.* The ITAA introduced a penalty of up to three years imprisonment or fine or both if a person "fraudulently or dishonestly make[s] use of the electronic signature, password, or other unique identification feature of any other person."

[302] *See* Greenleaf, *supra* note 298, at 61. Reasonable security practices and procedures are defined as "practices and procedures designed to protect information from unauthorized use, modification, disclosure, or impairment."

[303] *See* Oqvuist, *supra* note 298*; see* Greenleaf, *supra* note 298. The ITAA enlarges government surveillance powers, giving the government the power to "intercept data, access stored data, require retention of data and control encryption." *Id.* at 51. It may be the case that a normal consumer who brings a claim may not have a claim compatible with the government's standard. *Id.* at 61.

> Any person who sends, by means of a computer resource or a communication device-
> (a) any information that is *grossly offensive or has a menacing character*; or
> (b) any information which he knows to be false, but for the *purpose of causing annoyance, inconvenience*, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device; or
> (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or mislead the addressee or recipient about the origin of such messages, *shall be punishable with imprisonment for a term which may extend to three years and with fine*.[304]

Without substantial debate in the Indian Parliament, Section 66A, at the outset, was aimed at curtailing widespread misuse within popular modes of mass communication, including texting and emailing.[305] However, upon passage, commentators regarded the legislation a product of "shoddy drafting. . .completely at odds with the constitutional guarantees to freedom of speech and expression."[306] As individuals used Facebook and Twitter to project their dissent over alleged abuse of power in the country,[307] police started to arrest people indiscriminately, including a university professor, cartoonist, and businessman involved in the dissemination of cartoons and tweets portraying the decadence of Indian political life. [308] Moreover, two Mumbai residents were arrested posting

---

[304] IT ACT 2008, *supra* note 299.

[305] Olina Banerji, *Section 66A and Free Speech in India*: *The Debate Continues*, LONDON SCH. OF ECON. & POLI. SCI. (Jan. 30, 2013), *available at* http://blogs.lse.ac.uk/indiaatlse/2013/01/30/section-66a-and-free-speech-in-india/.

[306] Apar Gupta, *Problems are with Sec. 66A and not with its Implementation*, INDIA L. & TECH. BLOG (Nov. 26, 2012), *available at* http://www.iltb.net/2012/11/problems-are-with-sec-66a-and-not-with-its-implementation/.

[307] *Id.*

[308] H.S. Gill, *Information Technology Act Section 66(a)*: *An Analysis*, INDIAN STRATEGIC STUDIES (Jan. 27, 2013), *available at* http://strategicstudyindia.blogspot.com/2013/01/information-technology-act-section-

"offensive comments" on Facebook directed at leaders in the Indian Congress.[309] Section 67 also contained elements of ambiguity, particularly in the context of "preservation and retention" of data by intermediaries. In this section, an "intermediary shall preserve and retain such information as *may be specified* for such duration and *in such manner and format as the Central Government may prescribe.*"[310] Issues have also arisen with Section 69 in relation to the individual's right to encrypt data to safeguard his or her information from unwarranted state interference.[311] According to Section 69, an individual who refuses to heed to a government agency request to "access or secure access to a computer resource or fails to follow a government order to decrypt certain information" is subject to a seven year prison sentence.[312] Even more invasive, under Section 69B and its counterpart Section 70B, the Indian Government installed umbrella provisions covering data collection. To enhance "cybersecurity," Section 69B gives the Indian Government the power to:

> authorize any agency of the Government to collect traffic data—any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or *any other information.*[313]

Furthermore, under Section 70B, the Indian Computer Emergency Response Team, under the aegis of the Indian

---

66a.html; *see It's Not Just The Government Which Misuses Section 66A,* TECH2 (Mar. 26, 2013), *available at* http://tech.firstpost.com/news-analysis/its-not-just-the-government-which-misuses-section-66A.

[309] Gill, *supra* note 308.

[310] IT ACT 2008, *supra* note 299.

[311] Geoffrey King, *On Internet Freedom, India's Perilous Trajectory,* COMM. TO PROTECT JOURNALISTS (Jan. 13, 2014), *available at* https://www.cpj.org/internet/2014/01/on-internet-freedom-indias-perilous-trajectory.php.

[312] IT ACT 2008, *supra* note 299.

[313] *Id.*

Government, is given broad functional powers in the area of cybersecurity:

> (a) collection, analysis, and dissemination of information on cyber incidents; … [and]
> (f) *such other functions* relating to cybersecurity *as may be prescribed*.[314]

In 2011, the Indian legislature hastily[315] implemented the Information Technology Rules 2011 (IT Rules of 2011): a compilation of cyber-laws drafted pursuant to authority granted by the IT Act of 2000 and designed to implement the existing ITAA.[316] The IT Rules of 2011 in particular enumerated a series of security guidelines for cybercafés,[317] including an enforcement mechanism to monitor user activity.[318]

---

[314] *Id.*

[315] Thomas Claburn, *India Adopts New Privacy Rules,* INFO. WEEK (May 4, 2011), *available at* http://www.informationweek.com/government/policy/india-adopts-new-privacy-rules/229402835. "Because the [IT] Rules [of 2011] implement[ed] existing law, [the rules] did not undergo a prolonged period of public comment and industry input that typically precedes the passage of a law." *Id. See* Bhairav Acharya, *Comments on the Information Technology Rules 2011,* CTR. INTERNET AND SOC. (Mar. 31, 2013), *available at* http://cis-india.org/internet-governance/blog/comments-on-the-it-guidelines-for-cyber-cafe-rules-2011. The rules are prone to litigation due to poor drafting…new rules should be developed "in concert with experts, professional organizations, and civil society in a democratic manner." *Id.*

[316] Manish Sinha, *Indian IT Rules: A Critical Overview* (Aug. 25, 2011), *available at* http://thoughts.manishsinha.net/post/9371815499/indian-it-rules-2011-a-critical-review.

[317] Acharya, *supra* note 315. Under Section 3.1, a cyber café "means any facility from where access to the internet is offered by any person in the ordinary course of business to members of the public." *Id.*

[318] *Id.* Cyber cafes under the new IT rules are required to register their facilities with a "registration agency" that issues a unique registration number. *Id.* India has weakened individual privacy through the following sections of the new IT rules:

> (1) Section 4.2 states that "the cyber café shall keep a record of the user['s] identification document by either storing a photocopy or a scanned copy of the document duly authenticated by the user and

3. Societal Responses to Authoritative Decision-Making

India typifies a classic collectivist society: a society that is less individualistic and more trusting of others.[319] Indian culture honors a joint family tradition, where a small household may hold several family members all living in close quarters.[320] Indian society, rooted in Hindu tradition, perceives privacy in more spatial terms, as evidenced by practices separating women from men in the house to preserve morality and modesty.[321] Malavika Jayaram, an Indian intellectual property lawyer and scholar, conducted a study on Indian attitudes towards the concept of privacy. Jayaram delineated the perspectives of the Indian people toward privacy into five separate

---

> authorized representative of [the] cyber café. Such record shall be securely maintained for … one year."
>
> (2) Section 4.3 states that in addition to submitting user identification, the user may be photographed by the Cyber Café using a web camera installed on the computers in the Cyber Café for [purposes of establishing the identity of] the user. Such web camera photographs… shall be part of the log register maintained in physical or electronic form."
>
> (3) Section 5.3 states that the cyber café owner shall be responsible for storing and maintaining backup of following log records for each access or login by any user of its computer resource for at least one year including history of websites accessed using cybercafé computer resources
>
> (4) Section 7 states that "an officer authorized by the registration agency is [permitted] to inspect the cybercafé and computer resource[s]" therein for compliance of the aforesaid rules. "The cybercafé owner shall provide every related document, registers, and any necessary information to the inspecting officer on demand."

Id.

[319] Ponnurangam Kumaraguru & Niharika Sachdeva, *Privacy in India*: *Attitudes and Awareness V 2.0*, INDRAPRASTHA INST. INFO. TECH. 2, 6 (2012) (India).

[320] *Id.* While in the United States information would be disclosed to a spouse or parent, in India, information is typically "shared among uncles, aunts, and cousins "resulting in "more routine sharing of personal information among a wider group of people." *Id.*

[321] Subjahit Basu, *Policymaking, Technology, and Privacy in India*, 6 THE INDIAN J. OF L. & TECH. 65, 71 (2010) (noting a line of Indian case law that places emphasis on the concept of "bodily privacy" rather than privacy to personal information).

categories:

> General understandings and Concerns about Privacy: it would appear that Indians largely saw privacy in terms of personal space, not information as such;
> Awareness of and Concerns about Privacy and Technology: Indians were not as aware of the risks arising out of technology, such as threats from biometrics or the online environment, as their US counterparts;
> Comfort Level of Sharing Different Types of Data: appear[ed] that respondents were largely comfortable sharing their age, email address, and health information with websites, which reflected a similar trend to their American counterparts;
> Trust in Business and Government: Indians exhibited an overwhelming willingness to trust organizations and the State with personal information. Research in the West has shown a correlation between privacy-concern levels and distrust in companies and government;
> Posting Personal Information: Respondents not perturbed about personal information or traveler information being [posted . . . including} personally identifiable information (first and last names, age, gender, point of boarding [a] train, destination, and seat number).[322]

Observers have interpreted these trends among India's public as a sign of India's rudimentary knowledge of technology.[323] Others

---

[322] Malavika Jayaram, *The Business of Privacy*: *From Privacy Anxiety to Commercial Sense*? *A Broad Overview of Why Privacy Ought to Matter to Indian Businesses*, 4 N.U.J.S L. REV. 567, 575 (2011).

[323] *Attitudes Toward Privacy: A Comparison of India and the United States*, FROST BROWN TODD (Feb. 2007), http://www.frostbrowntodd.com/resources-214.html. [hereinafter *Attitudes Toward Privacy*]. *See* Kevin P. Donovan & Carly Nyst, *Privacy for the Other Five Billion*, FUTURE TENSE (May 17, 2013), *available at* http://www.slate.com/articles/technology/future_tense/2013/05/aadhaar_and_other_developing_world_biometrics_programs_must_protect_users.html. India recently instituted a program called "Aadhaar," an ambitious project "aimed at capturing fingerprints, photographs, and iris scans of 1.2 billion residents with the assumption that a national identification program will be a key ingredient to empower poor and unprivileged residents." *Id.* Proponents of Aadhaar and other

have attributed the Indian public's liberal outlook on privacy as an outgrowth of the legislative process conducted within the Indian parliament.[324] Some commentators have noted that privacy legislation in India is given cursory treatment, pushed through in a hasty manner without considerable foresight.[325] Justifications

---

biometric programs are noted to work "quietly and quickly before opposition can form." *Id.* The emergence of Aadhaar is due in part to the "lack of public education and consultation, as well as the paucity of technical expertise to advise on the risks and pitfalls of surveillance technologies." *Id. See Understanding and Overcoming Barriers to Technology Adoption Among India's Micro, Small, and Medium Enterprises*, INTUIT, *available at* http://www.intuit.in/images/MSME%20White%20Paper_FINAL.pdf (last visited Oct. 13, 2013). "The adoption of technology has not filtered through India's multiple economic and social divides." *Id.* at 11. One of the groups existing within this divide are the "26 million strong micro, small, and medium enterprises (MSME), which constitutes one of the most critical sectors in India's development and will play a pivotal role in India's economic growth." *Id.*

[324] DR. YOGENDRA NARAIN, AN INTRODUCTION TO THE PARLIAMENT OF INDIA preface (Rajya Sabha Sec'y 4th ed., 2007), *available at* http://rajyasabha.nic.in/rsnew/Parliament_of_India.pdf. India's federal structure rests on a parliamentary form of government "where the executive is accountable to the legislature." *Id.* The Parliament of India is subdivided into three separate bodies: "(1) President of India, (2) the Rajya Sabha (Council of States), and (3) the Lok Sabha (House of the People)." *Id.* The government introduces legislative proposals "in order to fulfill the promises for which it has received the mandate of the people." *Id.* at 18. Parliament also functions as a forum to "ventilate people's grievances." *Id.*

[325] *See* Datta, *supra* note 3. As a developing country, India has not instituted safeguards against the government or law enforcement agencies from having access to all private data of customers who engage in business with companies present in India. *Id.* For example, the Indian Parliament ratified the Information Technology Act of 2008 with "little debate and gave the government sweeping power to tap all communications without court order or warrant." *Id.* The author displays concern over the Parliament's passage of the Information Technology Act of 2008 by noting Section 69:

> Section 69 empowers the Central Government/State Government/its authorized agency to intercept, monitor, or decrypt any information generated, transmitted, received or stored in any computer resource if it is necessary or expedient so to do in the interest of sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offense or for investigation of any offense.

Id.

offered for the disconnect between the Indian legislature and more effective privacy legislation include that (1) privacy infringement has been a rare occurrence in modern Indian history;[326] (2) there is minimal public disapproval to the idea of centralized government;[327] and (3) "given the population density,[328] privacy is not a great concern."[329] Indicative of this view on privacy, the Indian parliament

---

[326] *Attitudes Toward Privacy*, *supra* note 323. *See* Apar Gupta, *Balancing Online Privacy in India*, 6 INDIAN J. L. & TECH. 43, 50 (2010). There is a claim that "Indian courts have not had the [opportunity] to adjudicate upon issues of information processing as it seems to not have been averred." *Id.* However, Indian persons "when alleging a breach of privacy are more concerned with the interception and dissemination of private information and seemed to have glossed over agitating about their rights against information processing." *Id.*

[327] *Attitudes Toward Privacy*, *supra* note 323; INDIA: FOREIGN POLICY AND GOVERNMENT GUIDE 31 (2011). The Indian Constitution has "fostered a steady concentration of power in the central government." *Id.* This movement toward greater concentration is a product of tensions between ethnic and caste groups across Indian society, in which the government has "resort[ed] to the formidable array of authoritarian powers provided by the Constitution." *Id. See* Nirvikar Singh, *The Dynamics of Reform of India's Federal System*, SANTA CRUZ CTR. INT'L ECON. (Mar. 2007), *available at* http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.226.4816. In the formative years of the Indian Constitution, concentrated power within the government proved effective as "interstate and center-state conflicts were resolved within [the Indian National Congress."] *Id.* at 3. The "national Indian bureaucracy" is accorded constitutional legitimacy and "there are provisions for independent bureaucracies in each state." *Id.* The reaction among the Indian people seems to reflect the historical importance of centralized government in Indian society. *Id.*

[328] *Attitudes Toward Privacy*, *supra* note 323; *see* Barbara Crutchfield George et al. *Offshore Outsourcing to India by U.S. and E.U. Companies: Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business Process Outsourcing*, U.C. DAVIS BUS. L.J (2006), *available at* http://blj.ucdavis.edu/archives/vol-6-no-2/Offshore-Outsourcing-to-India.html. The author suggests that the Indian parliament would have no compelling need to address privacy concerns when "approximately 1.1 billion people [are confined within] a geographical space one-third the size of the United States." *Id.*

[329] *Attitudes Toward Privacy*, *supra* note 323. A study conducted to assess Indian privacy outlooks found that "when asked what they thought of the statement 'data security and privacy are not really a problem because I have nothing to hide,' 89% of the Indian subjects agreed," which indicates the value Indian society accords to personal data protection. *Id.*

has taken few steps toward addressing feeble[330] enforcement mechanisms which are incapable of redressing individuals for data protection breaches.[331] Particularly, the civil and criminal systems[332] in India are plagued by procedural roadblocks that complicate efforts toward constructing a complete and accurate testimonial of individual concerns.[333]

One area noticeably affected by the uncertain privacy infrastructure and at risk of being subsumed by the growing surveillance state in India is the outsourcing industry. The Indian outsourcing industry is composed of approximately ten million people[334] supervising an extensive array of sensitive data consisting of "financial records, account information, and medical records."[335] Some observers have indicated that the security of this information is likely jeopardized considering the Indian IT sector has not fully

---

[330] Vinita Bali, *Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?* (Santa Clara Univ. Sch. Law Working Paper No. 06-10, Oct. 2006), *available at* http://ssrn.com/abstract=932679. "The existing enforcement regime in India's legal system is pitifully deficient, marred by interminable delays in moving matters through the court system." *Id.* at 5-6. India needs to provide a system to "expediently prosecut[e] data protection breaches and compensate those harmed." *Id.* at 6.

[331] *Id.* at 38. "Inefficien[t] court administration denies timely access to legal dispositions and gives litigants excessive control over persons seeking damages… and puts those persons in an unequal position by abusing and delaying the resolution procedures with impunity." *Id.*

[332] *Id.* at 39. Indian court proceedings are commonly recorded "by a judge who summarizes testimony for a court reporter," which contributes to the loss of "specificity, precision, and detail." *Id.* Moreover, "a case will not likely appear before the same judge for the duration of the its cycle: [judge] transfer occurs [at] a more expedient pace than judicial resolution." *Id.*

[333] *An Overview of Delay in Judicial System*, MAHESHWARI & CO., *available at* http://www.maheshwariandco.com/repository/articles/downloads/delay_in_judicial_system.pdf. The author mentions contributors to judicial delay in India, "including lacunae in the criminal procedure code, methods of police investigation, general administrative disorganization, and lack of modern technology." *Id.*

[334] IT & ITeS Industry in India, INDIA BRAND EQUITY FOUND. (Dec. 2013), *available at* http://www.ibef.org/industry/information-technology-india.aspx.

[335] Ponnurangam Kumaraguru & Lorrie Cranor, *Privacy in India: Attitudes and Awareness*, CARNEGIE MELLON UNIV. (2005), *available at* http://lorrie.cranor.org/pubs/PET_2005.pdf.

grasped the concept of privacy issues occurring within the industry.[336] Others have remarked that the absence of a proactive approach toward data security is a byproduct of the workplace environment, which has invested little in the well-being and quality of life of the IT worker.[337] As a result, the level of commitment and

---

[336] *See* Indu Nandakumar & Akanksha Prasad, *Outsourcing-shy: India Inc. like Wipro, ITC, Vedanta Prefers In-House Technology Teams*, THE ECON. TIMES (Oct. 3, 2012), *available at* http://articles.economictimes.indiatimes.com/2012-10-03/news/34238765_1_indian-companies-labour-arbitrage-cost-savings. Even though India has "pioneered the concept of information technology outsourcing,… Indian companies are yet to fully understand outsourcing." *Id.* Some Indian state-owned companies are hesitant to outsource based on a fear of "losing control over their business processes and sensitive data." *Id. See* DSCI-KPMG SURVEY: STATE OF DATA SECURITY AND PRIVACY IN THE INDIAN BPO INDUSTRY (2010), http://www.kpmg.com/IN/en/IssuesAndInsights/ThoughtLeadership/KPMG_DSCI_Data_Security_Privacy_Survey_2010.pdf [hereinafter DSCI-KPMG]. BPO stands for Business Process Outsourcing. "Only 50 percent of organizations that involve their legal department in the initial stages of contract negotiation and maintain and inventory of contractual/regulatory requirements for each client relationship are well aware of legal and compliance requirements for each type of data element." *Id.* The surveyors in this report noted the lack of clarity among BPO organizations in relation to their obligations under the ITAA 2008..and the absence of "dedicated … privacy team[s] … to support privacy initiatives." *Id.* There has been a trend among Chief Security Information Officers (CISO) at BPO companies to move "away from security related operational tasks and becoming more involved in strategic activities." *Id.* Because of this departure, business managers who have to shoulder the onus of the responsibility have not yet fully "underst[ood] security requirements of the business." *Id.*

[337] *See* Saritha Rai, *Indian Outsourcing's Little Brother: In Decline or Just in Need of a Makeover*, TECH. REPUBLIC (Jul. 25, 2012), *available at* http://www.techrepublic.com/blog/cio-insights/indian-outsourcings-little-brother-in-decline-or-just-in-need-of-a-makeover/. There is a divide in India's outsourcing industry, specifically with regard to the "social positioning" of the BPO employee. *Id.* Commentators have cited a "talent deficiency" within the industry. *Id.* India has struggled to rebrand the face of the IT employee from one who deals with "night shifts and customer service to one who is specialized in various roles." *Id; see* Jai Gill, *India's Outsourcing Firms Must Boost Morale,* BLOOMBERG BUS. WEEK (Nov. 4, 2012), *available at* http://www.businessweek.com/articles/2012-11-04/indias-outsourcing-firms-must-boost-morale. Employment in a BPO firm was once sought after as a prestigious, lucrative opportunity. *Id.* However, many workers have opted for employment in banking, retail, and manufacturing. *Id.* The lack of consensus among workers in BPO regarding their loyalty and advocacy for their employment has caused concern among BPO company leaders. *Id. "*Three

fervor from the BPO workforce toward their employers has declined.[338] Internal instability occurring within the outsourcing firm is also matched by tenuous contractual arrangements between the foreign data exporter and Indian outsourcing company that outline the transmission process.[339] While parties can generally stipulate the choice of law to be governed by the contract, called the Master Services Agreement,[340] the particular circumstances associated in an outsourcing contract tend to disfavor the foreign firm.[341] This type of leverage has encouraged companies who engage

---

out of five employees do not understand their role in fulfilling their organization's mission and are unclear how they will grow [with]in the organization." *Id.*

[338] *Id*; *see* DSCI-KPMG, *supra* note 336. The study noted a "lack of seriousness among BPO employees in the "young age group." From this pool of employees, the surveyors noted "high attrition rates, which have posed considerable obstacles to the sustainability and management of data security and privacy." *Id.*

[339] Sonia Baldia, *Offshoring to India: Are Your Trade Secrets and Confidential Information Adequately Protected*, MAYER BROWN, *available at* http://www.mayerbrown.com/files/Publication/c4321838-f2ec-4fe5-990d-1ea497a7398b/Presentation/PublicationAttachment/5a87579c-8d2b-469d-ad3dbb95435fe6ff/ART_OFFSHORINGTOINDIA_0308.PDF (last visited Oct. 22, 2013). Due to the lack of statutory and legal protections regarding trade secrets in India, the parties define their respective roles through the contract. *Id.* at 10.

[340] *See* Aurelio Locsin, *Definition of Master Services Agreement*, HOUS. CHRON., *available at* http://smallbusiness.chron.com/definition-master-services-agreement-40141.html (last visited Oct. 21, 2013).

> A master services agreement … spells out most but not all the terms between the signing parties. Its purpose is to speed up and simplify future contracts. [They delineate] payment terms, delivery requirements, intellectual property rights, warranties, limitations, dispute resolutions, confidentiality, and work standards.

Id.

[341] *See* Manishi Pathak, *Legal Considerations When Outsourcing to India*, Outsource (Jul. 30, 2012), *available at* http://outsourcemagazine.co.uk/legal-considerations-when-outsourcing-to-india. The foreign firm has to contend with the following factors when negotiating the law of the contract:

> [Because] a major proportion of the services are rendered in India, consideration for the services will be received in India, and the Indian party may sign the contract in India, applicability of Indian laws cannot be excluded [from] the contract.

Id.

in outsourcing with India to be more risk-averse:[342] proceeding tentatively[343] in their transactions with Indian outsourcing companies out of concern for India's position on data confidentiality.[344] Moreover, the likelihood of obtaining a judgment arising from a breach of a data transfer contract is uncertain.[345] Three parties, not necessarily all party to the contract, have a stake in the data transfer from the Indian outsourcing company and data transferor: "(1) the data subjects; (2) the third parties to whom the data is re-exported by the importer; and (3) the data protection authorities."[346] If a breach occurs in such a contract, damages can only be recovered from a

---

[342] Mubashshir Sarshar, *Laws Relating to Data Protection in India*, NAT'L L. U. DELHI 13 (Jan. 2011), *available at* http://works.bepress.com/mubashshir/28. States with inadequate data protection laws, including India, use "alternative avenues and ad hoc solutions to procure and continue business transactions." *Id.* Without legislation providing sufficient legal assurances for personal data security, "any uncertainty regarding doing business with an Indian BPO is a matter of negotiation of the relevant contract using appropriate expertise and advice." *Id.*

[343] Margaret P. Eisenhauer, *Privacy and Security Law Issues in Offshore Outsourcing Transactions*, HUNTON & WILLIAMS (Feb. 15, 2005), *available at* http://www.outsourcing.com/legal_corner/pdf/Outsourcing_Privacy.pdf

In deciding whether to transmit data overseas, companies "must consider two legal perspectives. First, it must consider whether any laws in the country where the data originates will continue to regulate the data post transfer. Second, it must consider whether laws in the country where the data is processed give rise to any additional risks or benefits." *Id.*

[344] *See India-Data Privacy*, WHITE & CASE LLP (May 1, 2013), *available at* http://aipf-association.fr/iafp/sites/images/images/India%20DP.pdf. For example, with regards to the issue of "employee consent for cross-border data transfer," there is no legislation explicitly requiring such consent "prior to transferring personal data outside India." *Id.*

[345] *See* Pathak, *supra* note 341. In the event of a possible dispute between the parties, "the Indian party could approach an [Indian] court to seek appropriate relief and the court can entertain the dispute" by referring to the above factors. *Id.* This puts the foreign party into a quandary because many client companies are concerned over the Indian judicial system. *Id.* As a result, arbitration clauses are commonly inserted into the Master Services agreement, "with the seat of arbitration and the rules governing the arbitration proceeding located in another country." *Id.* However, foreign firms face a significant issue with arbitral awards as Indian law prescribes that these awards can "only be enforced in a competent court in India through the filing of an execution petition." *Id.*

[346] Sarshar, *supra* note 342, at 19.

party to the initial contract. [347] As a result, when weighing whether to transfer data to an Indian BPO, corporate entities are confronting increased transaction costs in the form of precautionary measures to avoid severe breaches.[348]

IV. Predictions for Informational Privacy Rights: A Grim Prospect in the Era of the Surveillance State

A. United States

Even as Snowden's disclosures of NSA surveillance continue to emerge and the United States has awakened to the ever-present danger of data security, the U.S. Government will likely experience further calls for transparency reforms and massive overhaul of the data surveillance regime currently in place. The social media giant Twitter has issued statements indicating "it is prepared to sue the Obama Administration for the right to disclose more details about government surveillance requests."[349] Twitter's head of global legal

---

[347] *Id. See* Baldia, *supra* note 156, at 10. Regardless if the parties enter into a contract, Indian law has no equivalent to the tort of "breach of confidence." *Id.* This is compounded by the fact that compliance with the duty of confidence is made difficult in the context of outsourcing because:

> The duty … can be enforced only against a party that is either a fiduciary to the customer or in an employer-employee relationship with the complaining party. Also, the duty arguably only extends to the unauthorized disclosure of confidential information to a third party and does not prevent the recipient's own "misappropriation" of the information…[e]ssentially, the customer is left without a direct remedy against the Indian [entity] and without an [effective] legal means to stop the disclosure.

Id. at 10.

[348] Michael L. Rustad & Thomas H. Koenig, *Extending Learned Hand's Negligence Formula to Information Security Breaches*, 3 J. L. & POL'Y FOR THE INFO. SOC'Y 236, 254 (2007). The firm that decides to outsource data must follow "due diligence both through inspection and staff training in offshore facilities in order to protect its outsourced data." *Id.* These measures are necessary given that "Indian call centers and data processors manipulate consumer data twenty-four hours a day, seven days a week." *Id.*

[349] *See Twitter Threatens to sue the Obama Administration*, THE HILL (Feb. 6,

policy claimed a recent meeting with the Justice Department did not adequately confirm the U.S. government's will to reaffirm its commitment to protecting the right to "free expression and open discussion of government affairs."[350] Officials from Twitter have further commented that the lack of transparency from Washington has impacted their consumer base as individuals are questioning the frequency of Twitter's data transfers to the federal government.[351] The U.S. military has forecasted the rise of advanced surveillance techniques that will mimic technologies found within Apple Co.'s device "Siri."[352] The Defense Advanced Projects Research Agency (DARPA), who pioneered the "Siri" technology envisions a society where "popular communications devices" used worldwide will "report every single interaction with [devices like] Siri, leaving them wide open to the NSA."[353]

As transparency issues continue to mount on the federal level, some states have taken affirmative steps in neutralizing surveillance concerns in their own communities.[354] Indiana House

---

2014), *available at* http://thehill.com/blogs/hillicon-valley/technology/197646-twitter-considers-legal-fight-to-disclose-docs.

[350] *Id.* The meeting held between the Justice Department and five tech companies, including Twitter, resulted in an agreement whereby the companies would "disclose when they receive[d] national security letters and Foreign Intelligence Surveillance orders, which force companies to turn over information about users." *Id.* The agreement, to the chagrin of Twitter, "only allows companies to report ranges of 250 to 1,000, depending on how they categorize requests." *Id.*

[351] *Id.* The author noted Twitter has received a "steady increase in the number of government requests for information … over the past two years … [with] about 59% percent of requests in the last six months of 2013 coming from the U.S…and 45 different countries have asked for information since 2012." *Id.*

[352] *See* Steve Watson, *DARPA Boffin: Future Government Surveillance Will be Like Apple's Siri,* INFOWARS (Feb. 7, 2014), *available at* http://www.infowars.com/darpa-boffin-future-government-surveillance-will-be-like-apples-siri/. The author notes there is a possibility that "NSA spooks will interact with algorithms that become smarter as they know what to expect." *Id.*

[353] *Id.*

[354] *States Look to Rein in Government Surveillance,* NEWSFACTOR (Feb. 6, 2014), *available at* http://www.newsfactor.com/story.xhtml?story_id=01200189VHIC&full_skip=1 [hereinafter *Rein in Government Surveillance*]. Bills are being formulated in 14 states, including a "Colorado proposal that would limit the retention of images from license plate readers, an Oregon bill that would

Bill 1009 recently passed the House and is now heading to the Senate for further review.[355] Under HB 1009, the police are required "to obtain a search warrant before using a phone to track a person's location or using an unmanned device—such as a drone—to gather information in most situations."[356] Moreover, the bill also limits police access to information stored on electronic devices, such as passwords, unless a warrant is issued.[357] A similar bill in Missouri would make electronic data immune from search and seizure.[358] To many cybersecurity commentators, the longevity of the Section 215 metadata program is an enigma. President Obama has suggested his administration would strip control of the program from the NSA and transfer the data to third parties, leading some experts to propose the NSA would likely proceed in its data collection efforts even though it no longer held the metadata.[359] Some foresee the establishment of a clearinghouse that would audit the Section 215 program and provide a vehicle to ensure some semblance of due process.[360] Since the NSA is a self-auditing entity, the establishment of a clearinghouse would require the NSA, if it submits a request to retrieve metadata, to give the clearinghouse personnel and its legal counsel an opportunity to assess whether the request is legitimate.[361]

The technology sector is undergoing a renaissance in sophistication and novelty that will likely continue for the near future. First, the "cloud computing" sector has become a popular

require "urgent circumstances" to obtain mobile phone location data, and a Delaware plan that increases privacy protections for text messages." *Id.*

[355] *Christmas in Schools, Digital Surveillance, Road Bills Move On*, INDYSTAR (Feb. 3, 2014), *available at* http://www.indystar.com/story/news/politics/2014/02/03/christmas-in-schools-digital-surveillance-road-bills-move-on/5191593/.

[356] *Id.*

[357] *Id.*

[358] *Rein in Government Surveillance, supra* note 354.

[359] Joel M. Margolis, Vice President of Government Affairs at Subsentio, Inc. (Intelligence Gathering Entity), *What is the Future of the NSA Metadata Program?-Why You Should Care*, SUBSENTIO (Jan. 20, 2014), *available at* http://www.subsentio.com/live/regulatory/joels-blog-time/safe-harbor-review-20140120/.

[360] *Id.*

[361] *Id.*

commodity for public and private sector organizations.[362] Cloud computing is a system enabling "ubiquitous, convenient on-demand network access to a shared pool of configurable resources. . .that can be rapidly provisioned and released with minimal management effort or service provider interaction."[363] By 2018, cybersecurity analysts project the United States will make an $18.4 billion investment in cloud computing.[364] Given Snowden's insight into the NSA's capabilities and the recent string of data privacy breaches occurring in credit card systems at widely popular retail outlets, including Target, the presence of amorphous cloud servers with little oversight will likely raise serious concerns for individual privacy and protection of sensitive data.[365]

B. India

The prospects for greater information privacy freedoms in India are in flux due to the Indian government's expansion of the surveillance state without adequate legislative authorization.[366] Three mechanisms indicate a trend toward a police-state in India. First, the Centralized Monitoring System (CMS)[367] initiated in 2009 by the

---

[362] Mitchell S. Kominsky, *The Current Landscape of Cybersecurity Policy: Legislative Issues in the 113th Congress*, HARV. NAT'L SEC. J. (Feb. 5, 2014), *available at* http://harvardnsj.org/2014/02/the-current-landscape-of-cybersecurity-policy-legislative-issues-in-the-113th-congress.

[363] *Id.*

[364] *Id.*

[365] *Id.*

[366] *See* Pranesh Prakash, *How Surveillance Works in India*, NY TIMES (Jul. 10, 2013), *available at* http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/. "No intelligence agency in India has been created by an Act of Parliament with clearly established roles and limitations on power…there is no public accountability whatsoever." *Id. See Legal Framework for NATGRID Project of India Needed*, CIV. LIBERTIES PROTECTION IN CYBERSPACE (Sep. 21, 2013), *available at* http://ptlb.in/clpic/?p=224. India's government "is not very interested in enacting laws that reconcile civil libert[ies] and national security requirements in India." *Id.*

[367] *See* Bhairav Acharya, *India: Privacy in Peril*, FRONTLINE (Jun. 26, 2013), *available at* http://www.frontline.in/cover-story/india-privacy-in-peril/article 4849211.ece. India plans to pursue the surveillance programs without "enabling

Indian government has gradually come to the fore as Indian cities have implemented the voice and data interception equipment into their telecommunications infrastructure.[368] CMS is expected to be operational by 2014.[369] An overarching surveillance system of this magnitude pursued without sustained public discourse foreshadows continued state dominance over the individual.[370] Second, the Aadhaar[371] program as of September 23, 2013, received a declaration by the Indian Supreme Court finding that the biometrics collection practices associated with the program are not compulsory for Indian citizens.[372] Despite the ruling, however, the Indian government has

---

legislation." *Id; see* Prasant Naidu, *With India's Prism "Central Monitoring System" Online Privacy is a Myth,* BUSINESS2COMMUNITY (Jun. 21, 2013), *available at* http://www.business2community.com/trends-news/with-indias-prism-central-monitoring-system-online-privacy-is-a-myth-0530321. CMS will enable the government "to monitor all phone and internet communications in the country…provid[ing] state bodies like the National Investigation Agency centralized access to [India's] telecom network," with the ability to oversee "all phone calls and text messages." *Id.* Furthermore, the Indian government is "working on tracking the exact location details of people during their calls." *Id.* CMS is justified on national security grounds and "security agencies will no longer need court approval for surveillance." *Id.*

[368] *Moving Toward a Surveillance State-India,* CTR. FOR INTERNET AND SOC. (Jul. 19, 2013), *available at* http://www.medianama.com/2013/07/223-moving-towards-a-surveillance-state-cis-india/.

[369] *Id.*

[370] Nandagopal J. Nair, *India's new surveillance network will make the NSA green with envy,* QUARTZ (Jun. 28, 2013), *available at* http://qz.com/99019/no-call-email-or-text-will-be-safe-from-indias-surveillance-network/. Absent a formal privacy law in India, CMS will "operate under the archaic Indian Telegraph Act of 1885." *Id. See* Jillian C. York, *NSA Leaks Prompt Surveillance Dialogue in India,* ELEC. FRONTIER FOUND. (Jul. 10, 2013), *available at* https://www.eff.org/deeplinks/2013/07/nsa-leaks-prompt-surveillance-dialogue-india. The Indian Telegraph Act stipulates that "interception must be time-limited and targeted." *Id.*

[371] Surabhi Agarwal, *The UID Crisis: Don't Waste It,* BUS. STANDARD (Oct. 2, 2013), *available at* http://www.business-standard.com/article/opinion/the-uid-crisis-don-t-waste-it-113100200840_1.html. The UID, Unique Identify or otherwise known as Aadhaar, has not taken into account various government agencies, which have linked with the program, to make sure they are protecting sensitive personal data. *Id.* A privacy bill attached to the UID to address these issues was presented three years ago and the bill continues to be amended. *Id.* Without some level of enforcement, privacy breaches are likely to continue. *Id.*

[372] *See Aadhaar Card Cannot Be Made Mandatory for Availing Public*

kept the essence of the program by pursuing a new law creating a National Identification Authority of India to make modifications to the Aadhaar program.[373] So it seems that India will perpetuate surveillance policies until the Supreme Court declares the entire program unconstitutional.[374] Third, the National Intelligence Grid (NATGRID),[375] proposed in 2011, is planned for its first data linkage within 18 months.[376] The Indian Home Ministry is currently planning to issue an executive order for NATGRID's implementation in order to strengthen the program's legal backbone.[377]

Through the aforesaid events, the movement toward government supremacy over information traveling through cyberspace is inevitable. Furthermore, a specter of doubt has been raised as to whether Indian outsourcing firms can maintain their longstanding position as a hub for economic activity overseas as a result of weak data protection enforcement. Neighboring Asian countries, including the Philippines are likely to supplant India for this coveted position.[378] The Philippines passed its own data privacy act with significant support from the executive branch to satisfy the

---

Services in India: Supreme Court, CLPIC (Sep. 24, 2013), *available at* http://ptlb.in/clpic/?m=201309 [hereinafter *Aadhaar Card*].

[373] *See Cabinet Gives Go-Ahead for Aadhaar Bill*, THE ECON. TIMES (Oct. 9, 2013), *available at* http://economictimes.indiatimes.com/news/economy/policy/Cabinet-gives-go-ahead-to-Aadhaar-Bill/articleshow/23762608.cms.

[374] *See Aadhaar Card*, *supra* note 372.

[375] *See* V. Balachandran, *NATGRID will prove to be a security nightmare*, SUNDAY GUARDIAN, *available at* http://www.sunday-guardian.com/analysis/natgrid-will-prove-to-be-a-security-nightmare. (last viewed Feb. 19, 2014). Under NATGRID, "ten central agencies will be able to electronically access 21 sensitive databases held in banks, credit cards, internet, cell phones, immigration, motor vehicle departments, railways, National Crime Records…and the Income Tax Department." *Id.* These databases will "own" the data and have its own "management hierarchy." *Id.*

[376] *See* Aman Sharma, *NATGRID to get legal powers soon*, THE ECON. TIMES (Sep. 10, 2013), *available at* http://articles.economictimes.indiatimes.com/2013-09-10/news/41938113_1_executive-order-national-intelligence-grid-databases.

[377] *Id.*

[378] *See* Alec Christie, *New Tough Data Privacy Regime in the Philippines: Data Privacy Act signed into law*, DLA PIPER (Jul. 17, 2012), *available at* http://www.dlapiper.com/global/publications/Detail.aspx?pub=7515&rss=true. There has been an "expansion of data privacy laws in the Asia-Pacific region." *Id.*

Filipino BPO's sector's need for data security.[379] The Filipino Data Privacy Act of 2012 (DPA) or Republic Act No. 10173 has established a "comprehensive framework for the protection of personal information while ensuring the flow of information to promote innovation and growth."[380] The DPA's provisions have received positive feedback from the business community due to the relative ease in complying with the law.[381] Furthermore, the Philippines have fostered a culture of data protection, where it is commonplace for public and private sector firms to strictly adhere to the client's requests for non-disclosure.[382] Because the Philippines seems to embrace the principles of personal privacy protection of sensitive data and has the societal foundation to sustain the integrity of the DPA, India may be at risk of losing its competitive advantage in the outsourcing arena.

---

[379] *How Philippines Got the Edge over India in the Outsourcing Industry*, BPM WATCH (Sep. 18, 2013), *available at* http://www.bpmwatch.com/columns/philippines-got-edge-india-outsourcing-arena/.

[380] FINANCIER WORLDWIDE: DATA PROTECTION & PRIVACY LAWS-ANNUAL REVIEW 60 (2013), *available at* http://www.financierworldwide.com/Annual Reviews/AR_Data_247str.pdf.

[381] *Id.* at 61.

[382] *Id.* at 63.

V. The Days of Anonymity are Gone: Appraisal and Recommendations Toward Sustaining Information Privacy Rights in the Surveillance State

A. Appraisal of Past and Future Trends in Decision

1. United States

The state of surveillance in the United States has reached an all-time high, the culmination of decades of political wrangling and failure to adapt security measures with the ever-increasing scope and breadth of technology today. At the same time, however, the presence of terrorism and other grave threats to our homeland mandate that our country's leaders use all the resources available, specifically in the intelligence arena, to prevent another catastrophic attack on our country. It is hard to conceive the United States, the most storied democratic nation on Earth, embarking on a path toward absolute surveillance many of the most brutal totalitarian governments have taken and ultimately failed in the end. Today, we are contributing to Foucault's panoptic state by engaging heavily in social media and in turn building a boundless digital world where personal data flows seamlessly between cultures, communities, and states. This society of extreme openness makes it ripe for the NSA to get an intimate feel for the ideas and philosophies that go against the grain in Washington. While understandably, social media is a burgeoning industry, generating unprecedented revenue for the pioneering companies, including Facebook and Twitter, and has figuratively become an appendage of the so-called "millennials,"[383] individuals have the power to discourage its use and find alternative means. Claims of data breaches and identity theft as mentioned in this article have arisen exponentially in part due to excessive reliance

[383] *See* Morley Safer, *The "Millenials" are Coming,* CBS NEWS (May 23, 2008), *available at* http://www.cbsnews.com/news/the-millennials-are-coming/. Millenials are referred to individuals "born between 1980 and 1995." *Id.* Safer describes this group as "tech savvy, with every gadget imaginable becoming an extension of their bodies…they multitask, talk, walk, listen, type and text." *Id.*

on social media with its limited protections. At the same, the United States has to think one step ahead of its enemies. The margin for error among intelligence agencies is slim, and the fact remains that the NSA must locate threats and address risks before they metastasize.

2. India

Information technology commentators agree that something needs to be done to address the gaps in India's privacy framework.[384] These commentators have come to consensus that India:

> (1) has no comprehensive law and the privacy issue is dealt with proxy laws that do not converge on the privacy issue;
> (2) does not classify information as public information, private information, or sensitive information;
> (3) does not have a legal framework that talks about ownership of private and sensitive information and data;
> (4) does not have a certain procedure of creating, processing, transmitting, and storing the information;
> (5) lacks any guidelines that define data quality, proportionality, and data transparency.[385]

India's constitutional and statutory standards for basic privacy protections, as espoused through Article 19 and 21 of the Indian Constitution and the IT Act are overtly deferential to the government and do not adequately provide sufficient guarantees to the Indian people that there exists a clear separation between private and public matters. Given India's geographical location, amidst sectarian volatility and terrorism in neighboring Pakistan and Afghanistan, and fears of this instability flowing into the country, India's government has not found the appropriate balance between

---

[384] Shrikant Ardhakapur et. al., *Privacy and Data Protection in Cyberspace in Indian Environment,* 2 INT'L J. ENG'G SCI. & TECH. 942, 943 (2010).

[385] *Id.*

maintaining some semblance of freedom of expression while securing the country from its archenemies. Instead, the Indian government is looking to suppress the external forces lying beyond its borders instead of carving a viable path for the Indian people to prosper. The presence of two emerging surveillance apparatuses—NATGRID and CMS—that capture electronic communications and locate individual movements are clearly an impediment toward reversing this trend. Both programs subvert proper legislative approval, contain no meaningful benchmarks for accountability and transparency for their controllers, and exist in the presence of a frail privacy regime that can do little to deter its intrusive behavior.

At the same time, the collectivist spirit cherished by the Indian people is vulnerable to attack, as the cultural tendency to share information amongst friends, family, and peers has confronted an impregnable wall of regulation that aims to censor views that are deemed provocative or grossly offensive. What is offensive according to the Indian government is ambiguous and not clearly delineated in the initial IT Act and its 2008 amended version. Without a standard to assess offensive conduct in electronic communications, innocent Indians are being arrested or prosecuted and otherwise lawful speech is being removed without any notice or opportunity to be heard. Despite its status as the world's largest democracy and a platform for global communication technology, India is struggling to respond to a growing sector of its population that relies exclusively on social media to comment on the rather lopsided political establishment in Delhi. To compensate for its poorly-crafted laws that do little to rally public confidence in the government's endeavors to defend personal privacy protections and freedom of expression, India is ratcheting up its surveillance techniques to mitigate the effect of information that can travel in real-time and possibly threaten instability in the country. The state of data privacy in Indian outsourcing is just a microcosm of the broader cultural and political problem with privacy standards and allowing individuals and entities to keep their information confidential. With no comprehensive data protection legislation in place to address novel cybercrimes, the Indian outsourcing industry remains a magnet for security breaches.

3. Comparative Evaluation

India and the United States are part of a new technology phenomenon. Today, both countries are traveling down this treacherous, Orwellian road to absolute surveillance without a comprehensive law to address the ability of various stakeholders to access and analyze data in large quantities. Both the Information Technology Act of 2008 and the Foreign Intelligence Surveillance Act as well as their respective amendments contain cryptic language, often grossly overbroad or vague as to suggest an alternate meaning outside the text of the law itself and in hidden opinions, usually found in classified documents outside the public domain. This lack of clarity in both countries, justified mainly on grounds of national security and foreign intelligence collection, raises serious transparency issues as to the merits of these practices and the criteria the government uses to determine which data comports with the these standards. In terms of "systematic access to stored data" the United States responds in this fashion:

> A special court [The Foreign Intelligence Surveillance Court (FISC)] orders telecommunications service providers to disclose to the National Security Agency, on a daily basis, metadata for all telephone calls handled by the carriers to and from the country. The bulk disclosure orders have to be renewed every 90 days. . .[386]

Similarly, India's future Central Monitoring System (CMS) will provide the Indian government the ability to "engage in real-time interception of email, chats, voice calls, and texting, without intervention of the service providers."[387] When viewed in the absence of privacy legislation or regulation over the cloud, the

---

[386] Ira Rubinstein, et al., *Systematic Access to Personal Data*: *A Comparative Analysis*, CTR. DEMOCRACY & TECH. 5 (Nov. 13, 2013), *available at* https://cdt.org/files/pdfs/govaccess2013/government-access-to-data-comparative-analysis.pdf.

[387] *Id.* at 6.

likelihood for data breaches in India grows exponentially. Here, India is far more sweeping in its collection endeavors, as the CMS will not differentiate between content and metadata whereas the United States has FISA and the ECPA, which require a subpoena to collect metadata and internet data with a court order. Furthermore, India's perspective on surveillance is sweeping instead of being case-specific, as the government and its newly crafted CMS will not differentiate between information used for law enforcement or national security purposes. India can learn from the United States, which has delineated access to information for law enforcement purposes (ECPA) and for foreign intelligence activity (FISA).[388]

The United States, through its Privacy and Civil Liberties Oversight Board (PCLOB), boldly presented a lengthy commentary into the drawbacks and implications of the NSAs data collection programs "so that the public and Congress can have a long and overdue debate about the privacy issues raised."[389] Conversely, following Snowden's disclosures, India did not seriously address the reality of surveillance in its own domestic agenda but instead put CMS, NATGRID, and other ambitious programs on the fast track. This prioritization of interests indicates that India may not be invested in elevating the rights of the individual ahead of the government. This is also a reflection of the lack of technical understanding among a vast majority of Indian people. While there is some concern over the range of access to data, this concern has not, as of yet, risen to the level of establishing a formal board to discuss these matters openly and honestly.

---

[388] *Id.* at 26.

[389] PRIVACY AND CIV. LIBERTIES OVERSIGHT BD., *supra* note 196, at 1.

B. Recommendations

1. United States

Seven months following Snowden's disclosures, the PCLOB enumerated a groundbreaking list of recommendations to further the discourse on reining in the surveillance state from government abuse.[390] The PCLOB stated that the U.S. government "must take the initiative and formulate long-term solutions that promote greater transparency for government surveillance policies more generally, in order to inform public debate on technology, national security, and civil liberties going beyond the current controversy."[391] In particular, the PCLOB recommended the following 12 actions:

> (1) the U.S. Government should discontinue the Section 215 bulk collection program on the grounds that alternative means exist legally to acquire pertinent data without bringing individuals not affiliated with terrorism or criminal elements into the fold;[392]
> (2) the U.S. Government immediately institute privacy safeguards to Section 215 namely:
> a) reducing the retention period for bulk telephone records program from five to three years;
> b) reducing the number of "hops" used in contact chaining from three to two;
> c) submit the NSAs "reasonable articulable suspicion" determinations to the FISC for review after they have been approved by the NSA and used to query the database; and
> d) require a "reasonable articulable suspicion" determination before analysts may submit queries to, or otherwise analyze, the "corporate store" which contains the result of contact chaining queries to the full "collection

[390] For a brief description of the PCLOB, *see* PRIVACY AND CIV. LIBERTIES OVERSIGHT BD., *supra* note 196. The board spoke on January 23, 2014 regarding the NSA bulk collection program and a list of recommendations desired from the executive to quell concerns over NSA's overreach into personal data.

[391] *Id.* at 15.

[392] *Id.* at 16.

> store."[393]
>
> (3) Congress should enact legislation enabling the FISC to hear independent views, in addition to the government's views, on novel and significant applications and in other matters which a FISC judge determines that consideration of the issues would merit such additional views.[394]
>
> (4) Congress should expand appellate review for FISC opinions by providing a role for the Special Advocate to seek that appellate review, thereby bolstering confidence in the integrity of the process.[395]
>
> (5) The FISC should take full advantage of existing authorities [special masters or other technical experts] to obtain technical assistance and seek input from outside parties.[396]
>
> (6) To the extent provided by national security, the government should create and release with minimal redactions declassified versions of new decisions, orders, and opinions by the FISC in cases involving novel interpretations of FISA or other significant questions of law, technology, or compliance.[397]
>
> (7) Regarding previously written opinions, the government should perform a declassification review of decisions, orders, and opinions by the FISC that have not yet been released to the public and that involve novel interpretations of FISA or other significant questions of law, technology, or compliance.[398]
>
> (8) The Attorney General should regularly and publicly report information regarding the operations of the Special Advocate program recommended by the board. This should include statistics on the frequency and matters of Special Advocate participation in FISC proceedings.[399]

---

[393] *Id.* at 17.

[394] *Id.* This "special advocate" would make "legal arguments addressing privacy, civil rights, and civil liberties interests and review the government's application…as to whether the proposed surveillance or collection is consistent with law or unduly affects privacy and civil liberties interests." *Id*. at 18.

[395] *Id.* at 18.

[396] *Id.*

[397] *Id.*

[398] *Id.* at 19.

[399] *Id.*

> (9) The government should work with Internet service providers and other companies that regularly receive FISA production orders to develop rules permitting the companies to voluntarily disclose certain statistical information. In addition, the government should publicly disclose more detailed statistics to provide a more complete picture of government surveillance operations.[400]
> (10) The Attorney General should inform the PCLOB of the government's activities under FISA and provide the PCLOB with copies of the detailed reports submitted under FISA to the specified committees of Congress. This should include providing the PCLOB with copies of the FISC decisions required to be produced under 50 U.S.C. § 1871(a)(5)[requires the congressional intelligence and judiciary committees to be provided with decisions, orders, and opinions from the FISC, and from its companion appellate court, that include significant construction or interpretation of FISA provisions].[401]
> (11) The Board urges the government to begin developing principles and criteria for transparency, specifically as to what can be kept secret and what can be released as to existing and future programs that affect the American public.[402]
> (12) The scope of surveillance authorities affecting the American public should be public, with regard to the government's interpretation of statutes that provide for ongoing surveillance programs affecting Americans.[403]

At the behest of the PCLOB and its calls for significant reforms to the NSA bulk collection program, President Obama issued a speech at the Department of Justice on January 17, 2014.[404] President Obama noted the "inherent potential for abuse in massive

---

[400] *Id.*

[401] *Id.* at 20.

[402] *Id.*

[403] *Id.*

[404] *See* Fred Kaplan, *Pretty Good Privacy: The Three Ambitious NSA Reforms Endorsed by Obama, and the one he rejected*, SLATE (Feb. 7, 2014), *available at* http://www.slate.com/articles/news_and_politics/war_stories/2014/01/obama_s_nsa_reforms_the_president_s_proposals_for_metadata_and_the_fisa.html.

data-gathering" but affirmed that "metadata collection is not going away" anytime soon.[405] To address uncertainty over the NSA's capability of effectively shielding information collected from continued misuse, President Obama stated he would prevent the NSA from accessing the information and would consider transferring control of the data to an unspecified third party.[406] This procedure would require the NSA to use the FISC's procedural framework to retrieve the data.[407] Furthermore, President Obama desired to limit effective immediately the "number of hops the NSA can make in fanning out its surveillance from three to two."[408] This would minimize the amount of people that could be under the microscope when a single individual is tracked.[409] Finally, with regard to the composition of the FISC, President Obama did not seek to divest the Chief Justice of the Supreme Court of his power to select judges.[410] However, President Obama accepted the inclusion of a "privacy advocate that can make a case for turning down a request based on civil liberties."[411] On February 6, 2014, the FISC, in accord with President Obama's recommendations given on January 17, commenced preparations for compliance with the requests.[412] As conveyed by the Office of the Director of National Intelligence (ODNI), the FISC agreed to modify the 215 program to guarantee that "metadata will only be queried after a judicial finding that there is a "reasonable, articulable suspicion" that the selection is associated with an international terrorist organization" absent a true

---

[405] *Id.*

[406] *Id.*

[407] *Id.*

[408] *Id.*

[409] *Id. See Office of Press Secretary: Remarks by the President on Review of Signals Intelligence*, WHITEHOUSE.GOV (Jan. 17, 2014), *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

[410] *See* Kaplan, *supra* note 404.

[411] *Id.*

[412] *See* Andrea Peterson, *Obama Administration Starts to Implement Changes to NSA Phone Records Program*, WASH. POST (Feb. 7, 2014), available at http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/07/obama-administration-starts-to-implement-changes-to-nsa-phone-records-program/.

emergency."[413] Furthermore, the FISC planned to "[limit] the query results to metadata within two hops of the selection term, rather than the prior three."[414]

However, in light of Obama's ambitious privacy reforms, the continuing innovation occurring within the high tech industry and the acquisition of new technologies by rogue regimes, including Iran and North Korea, makes it highly unlikely the NSA will temper its collection at the expense of preserving U.S. national security interests. To prevent another Snowden incident, oversight committees within each intelligence agency should become more prevalent. Although this method would not create a comfortable workplace environment for intelligence employees, this high caliber level of supervision would ensure accountability and transparency. If any intelligence employee is caught attempting to release data, the agency should immediately terminate the employee and the employee should be criminally prosecuted.

For the normal citizen not toiling in the world of intelligence and sensitive data, there should be a better understanding into how information is being processed. This does not mean that intelligence agencies are obligated to spell out the exact minutiae of their particular endeavors, which would certainly jeopardize our interests at home and abroad, but instead delineate whether the information is being used for national security reasons or used for mere domestic criminal investigations. A statement should be given by a government official, in writing, citing the use of the information and its ultimate destination. If there is an egregious breach, such that the information collected amounts to a social security number or confidential record, then that person should have the right to a hearing or at least receive an affidavit from a government official certifying the collection will not adversely affect the individual.

Today, reports that have surfaced regarding the IRS' targeting of conservative groups arguably based on political ideology warrants an expeditious method of providing redress to compensate for any losses incurred by the targeting. Such redress should be

---

[413] *Id.*

[414] *Id.*

administered far away from the bureaucratic morass in Washington. In the case of the IRS, any kind of complaint over a tax-related inquiry, where personal information is sought, should be filtered through a neutral privacy oversight board composed of individuals in the private and public sector to determine the extent of the breach. This neutral privacy oversight board should be the liaison between the individual and the government. Its function should concentrate on specifically notifying federal law enforcement officials if there is concrete proof that a certain agency has deliberately manipulated or mishandled critical personal data that affects the livelihood of normal individuals.

Due to the severity of this issue and the extraordinary growth of the federal government, communities should create grassroots organizations devoted to personal data transparency. These groups should operate under the banner of reforming government ineptitude with respect to the data rights of individuals. Members of these groups should vigorously petition their senators and congressman, and establish satellite headquarters at each state capitol and at Capitol Hill, to push for the creation of a more comprehensive federal statute criminalizing intentional or grossly negligent mishandling of personal data. This statute would have a timing element attached to it, whereby the failure of a government agency to respond to a citizen complaint with 30 days entitles the person to monetary damage and a hearing. This level of response is necessary to bring about a gradual decentralization of power from Washington to the states and give the American people more certainty that they are not being watched, judged, or penalized on a daily basis.

2. India

Even though national security is one of India's primary justifications for using surveillance and may be well-intentioned, India should focus on strengthening its national security through greater privacy protections. The Indian government has shown its inability to promulgate meaningful, targeted reforms in the field of information privacy. The laws that have been passed harp on technicalities and arcane terminology, but do not provide comment on their efforts to protect the dignity of the individual. Respect for human dignity should be the responsibility of the Indian states themselves as they are already autonomous in nature.[415] The Indian states are more likely to have an intimate knowledge of the demographics of their territory and the concerns of their communities. There is no question that the surveillance state will subsume the most innocent of the Indian population; those individuals falling below the poverty line with low literacy rates.[416] Individual states should coordinate grassroots effort in various towns, villages, and municipalities to promote a sense of civic participation. Privacy committees should be established under the direction of the state governments. These committees should be composed of IT lawyers and technical experts that can explain complicated provisions in India's current data privacy legislation to ordinary individuals in rudimentary terms as well as any accompanying rights they may have in case of a breach. These privacy committees can also shift the cultural perception of privacy by promoting confidentiality agreements and the rights that flow from such agreements. Standard guidelines for preserving confidential information should be drafted by the privacy committees

---

[415] *See* U.S. DEP'T OF STATE, BUREAU DEMOCRACY, HUM. RTS. & LAB: INDIA EXECUTIVE SUMMARY 1 (2011), *available at* http://www.state.gov/documents/organization/186675.pdf. India includes "28 states and seven union territories [that] have a high degree of autonomy and have primary responsibility for issues of law and order." *Id.*

[416] *See* Donovan & Nyst, *supra* note 323. The Indian government is assuming that the poor and unprivileged will react positively the program, but there is little education occurring on the details of the program. *Id.*

and sent to local government responsible for handling sensitive data. These guidelines should require the formation of a binding written agreement between government employees and the individuals who transfer personal information to them on a daily basis. The agreement should stipulate that any information acquired will be protected from disclosure and any breach of the agreement would give the individual recourse in a court of law.

India's outsourcing companies are on the brink of losing their services to neighboring countries that are progressing toward more comprehensive privacy reforms. The lack of a privacy culture in India is a driving factor toward the movement of goods and services away from India. At its most basic level, BPO employees must be held accountable for any leaks that occur during a typical transaction with an overseas company. BPOs should draft a handbook containing easy to understand provisions that must be signed before employment commences. These provisions should focus on data handling and impose severe consequences for instances of data theft or transmission of data to unknown third parties. Since data protection law in India is an evolving process and changes to the law are bound to occur, the BPO should perform monthly training sessions to reiterate the importance of compliance with the rules. The training session should also update the employees on amendments to data protection laws in the United States, Europe, and other major centers. Finally, the current IT laws stemming from the IT Act of 2000 and its amended versions in 2008 and 2011 should increase personal liability among corporate officers, directors, and senior officials. The goal toward improving the dignity of the individual in the context of complicated regulations cannot be achieved without building a foundation of accountability for those directly involved in the transit of data overseas.

Conclusion

For now, the growth of mysterious, government-run programs will likely make private matters a thing of the past. The most challenging task for the individual is to demand accountability and answers from those in charge. Until a massive outpouring of criticism is leveled by the population toward the government, we can be assured that the surveillance state will grow at an astounding pace in the near future.