PRIVACY IMPLICATIONS OF BIG DATA AND PREDICTIVE ANALYTICS

By

Robert Sprague*

Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves.[1]

[T]he volume of information that people create themselves—the full range of communications from voice calls, emails and texts to uploaded pictures, video, and music—pales in comparison to the amount of digital information created *about* them every day.[2]

I. INTRODUCTION

Predictive analytics use a method known as data mining to identify trends, patterns, or relationships among data, which can then be used to develop a predictive model;[3] in many cases attempting to predict behavior. The advent of ubiquitous monitoring and tracking—from self-generated content, web browsing, online transactions, geolocation tracking, and infrastructure sensors—provide the "big data" needed for data mining and predictive analytics. Privacy law has not kept up, particularly since most of the data are "public" in that they are not secret or confidential. Yet, big data mining can reveal intimate facts and portrayals of individuals.

Besides providing general background on data analytics, this paper reveals that for all practical purposes it is impossible to avoid "emitting" digital information that can be collected, stored, analyzed, and used for a myriad of decision scenarios; all one can really do is be aware that it occurring—just about everywhere, just about all the time. This paper then explores possible theories of privacy protection for predictive analytics; specifically under the evolving "mosaic" theory that has so far been considered, to varying degrees, in Fourth Amendment search scenarios. This paper makes an argument that predictive analytics are ripe for privacy protection based on the mosaic theory.

* J.D., M.B.A. Associate Professor of Legal Studies in Business, University of Wyoming College of Business, Department of Management & Marketing.

Editorial Note: Throughout this paper, except perhaps within quoted text, data are referred to in their traditional plural nature; however, "big data" is generally referred to as a concept and is therefore singular.

II. PREDICTIVE ANALYTICS

Predictive analytics enable organizations to determine trends and relationships that may not have otherwise been readily apparent.[4] Increasingly sophisticated statistical models coupled with the growth of "big data"[5] have led to an increasing use of predictive analytics in a variety of situations.[6] The range of predictive analytics is bolstered by the vast amount of increasingly available data: online transaction records, email messages and metadata,[7] images, web browsing logs, search queries, health records, social networking interactions, geolocation tracking, and sensors deployed in infrastructure such as communications networks, electric grids, global positioning satellites, roads and bridges, as well as in homes, clothing, and mobile phones.[8] One can think of predictive analytics another way: "instead of people using search engines to better understand information, search engines will use big data to better understand people."[9]

But predictive analytics can go a step further than traditional data analysis—creating a picture of social behavior that was not previously possible.[10] Menchen-Trevino notes that a new interdisciplinary field, computational social science, is forming around the social analysis of digital imprints left by email, text messages, tweets, surfing the web, social media applications, and smart phones.[11] These data are not necessarily tracking transactional records of atomized behavior, such as the purchasing history of customers, but keeping track of communication dynamics and social interactions.[12] For computational social scientists, big data is "big" not because of its size but because its analytical potential is qualitatively different.[13] Indeed, some researchers claim that big data can track human behavior more precisely than theoretical models.[14] Big data can help illuminate the complexity that interactions add to social dynamics "with an impressive level of detail."[15]

Mayer-Schönberger and Cukier provide a brief analysis of the promise—and the peril—of big data predictive analytics. Prior to big data, analytics relied on determining whether an individual was part of a group; for example, actuarial tables indicate that men over fifty years of age are more prone to colon cancer, so all men over fifty may pay more for health insurance.[16] In contrast, big data analysis is noncausal, identifying individuals, rather than groups, from a vast array of data.[17] Mayer-Schönberger and Cukier argue that, on the plus side, this makes profiling much more accurate, less discriminatory, and more individualized.[18] For example, rather than identifying an individual as a terrorist threat due to his or her nationality or religion, additional data points, such as body language and other physiological patterns, can be analyzed to make a more accurate determination of a possible threat.[19] On the down side, it may lead some to predict behavior based on mere probabilities; big data analytics can only "predict that for a specific individual, a particular future behavior has a certain probability."[20]

Predictive analytics are not perfect. While they may reveal hidden correlations, there may be no causation. For example, Google engineers found a correlation between Google flu-related searches and outbreaks of the flu, identifying flu outbreaks before the Centers for Disease Control.[21] However, the engineers did not examine what caused those searches. For example, a few years later, Google's predictive capabilities came into question when it drastically overestimated peak flu levels based on search queries, most likely because Google's algorithms did not sufficiently take into consideration people who were not suffering from the flu conducting flu-related searches due to higher than usual press coverage of a flu outbreak.[22] "Imputing true causality in big data is a research field in its infancy."[23] In addition, while there may be a lot of data, they are not always complete or accurate and may contain outliers—all of which can lower the performance of data mining algorithms.[24]

III. PREDICTIVE ANALYTICS AND PRIVACY

In the early years of America as a colony and a nation, privacy was a relatively minor social concern in light of social norms: church elders would regularly visit the homes of parishioners to ensure proper living;[25] family members, as well as visiting guests, would often sleep in the same beds;[26] Henry Ford would send his "sociological investigators" to the homes of workers to ensure proper living before extending a wage bonus.[27] America's open frontier provided its own natural solitude.[28] Privacy was primarily limited to admonishing eavesdroppers—those who would stand outside the open eaves of a home and listen to the conversations within.[29]

When Warren and Brandeis proposed a "right to be let alone" in their seminal article *The Right to Privacy*,[30] it was in reaction to new intrusive technologies: "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[31] The latter half of the nineteenth century witnessed a change in society fueled by technological advancements, including the instant camera,[32] which itself helped fuel a profusion of newspapers and magazines satisfying an insatiable demand for gossip and intimate portrayals.[33]

Soon, "[a]cceptance of the right to privacy ha[d] grown with the increasing capability of the mass media and electronic devices with their capacity to destroy an individual's anonymity, intrude upon his most intimate activities, and expose his most personal characteristics to public gaze."[34] Now, in the twenty-first century, almost all aspects of modern life are digitally recorded, stored, and analyzed—the collection of information about us is ubiquitous.[35] Today, because of social media, mobile devices, surveillance devices, and networked sensors, individuals constantly emit information, whether they know it or not, that can be used or misused in a variety of ways.[36]

Most of the information we "emit" is digital (such as email and text messages, mouse clicks and keystrokes, phone numbers dialed and calls received, and GPS location data), which can suffer from over-collection and data fusion. "Over-collection occurs when an engineering design intentionally, and sometimes clandestinely, collects information unrelated to its stated purpose."[37] For example, does your smart phone camera record your facial expressions while it records your keystrokes when you type a text message?[38] In April 2014, the FTC filed a complaint against the maker of the "Brightest Flashlight App," a popular Google Android app that would activate all the lights on a mobile device, while also transmitting the device's geolocation to third parties, including advertising networks.[39] Data fusion occurs when data collected from different sources for different reasons are brought together, resulting in data-rich profiles and new ways of tracking.[40] "[T]he privacy challenges from data fusion do not lie in the individual data streams. . . . Rather, the privacy challenges are emergent properties of our increasing ability to bring into analytical juxtaposition large, diverse data sets and to process them with new kinds of mathematical algorithms."[41]

This is one way in which predictive analytics contribute to online tracking.[42] But one does not even have to shop online to be targeted by predictive analytics. Perhaps the most famous—and chilling—example comes from Target Corporation's use of analytics to predict its shoppers' future buying habits. Target, like all other retailers, understands that many consumer buying habits are ingrained and difficult to change.[43] One particular moment when buying habits

can change significantly is the birth of a child. However, most marketers are reactive—sending coupons and advertisements after the birth of the child based on public birth records. Target sought to be proactive—predicting when shoppers, based on buying habits,[44] are still pregnant.[45] Unfortunately, Target's analytics were so good it informed a father of his daughter's pregnancy before he even knew about it.[46] As the Target incident illustrates, predictive analytics can create a risk of revealing intimate personal information before it becomes publicly available,[47] even when the original data are non-personally identifiable.[48]

> Application of analytics to big data does not conform well to traditional legal approaches because big data does not result from one-on-one interaction between the data controller and the individual. Big data instead pulls in information from disparate sources. Its value derives not only from its volume, but also from its varied and expansive scope—big data brings together an enormous pool of information that initially may seem unrelated.[49]

A. The Public/Private Dichotomy and the Third-Party Doctrine

The principal privacy conundrum posed by predictive analytics is that data mining relies to a large extent on "public" information; it derives from transactions and social interactions that are often generally observable. "A matter that is already public or that has previously become part of the public domain is not private."[50] While total secrecy is not required—information disclosed to a few people may remain private[51]—still, if even only a few people actually see the information, privacy can be lost if the *potential* audience is large.[52] Parent expressly excludes information in the public domain from his definition of privacy, considering it a "glaring paradox."[53] Strahilevitz considers the boundary between public and private "*the* fundamental, first-principles question in privacy law."[54] And this public/private dichotomy is reflected in a number of court decisions: "objects, activities, or statements that [one] exposes to the 'plain view' of outsiders are not 'protected'";[55] "whatever the public may see from a public place cannot be private";[56] watching an appellee and videotaping his activities while he was outside his home, in his front yard, where he was exposed to public view was not an actionable invasion of privacy.[57] Indeed, one court has gone so far as to hold there was no reasonable expectation of privacy where a woman was recorded by a secretly installed camera while changing clothes in an office area, despite locking the door, because others had a key to the office and could have walked in at any moment.[58]

Closely related to the public/private dichotomy is the so-called "third-party doctrine," which provides that private information disclosed to a third party can lose its privacy protection. The doctrine originates in Fourth Amendment jurisprudence, particularly in: *On Lee v. United States*, in which the U.S. Supreme Court held there was no Fourth Amendment protection in a confidential conversation recorded by an informant;[59] *United States v. Miller*, in which the Supreme Court held that the Fourth Amendment does not require the government to obtain a warrant to seize bank records;"[60] and *Smith v. Maryland*, in which the Court held that dialed telephone numbers have no constitutional protection.[61]

The third-party doctrine is not without its critics.[62] One argument particularly germane to this paper is that privacy does not require total secrecy and that exposure to a limited audience does not equate to exposure to the world at large.[63] In contrast, Kerr argues the third-party doctrine prevents "savvy wrongdoers" from using "third-party services in a tactical way to enshroud the entirety of their crimes in zones of Fourth Amendment protection."[64] However, the

Supreme Court may ultimately recognize that modern technology may finally impose a limit on the Fourth Amendment's third-party doctrine:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.[65]

The third-party doctrine has been applied in common law privacy cases as well. For example, the United States District Court for the District of New Jersey dismissed a plaintiff's invasion of privacy claim against her employer in relation to restricted-access Facebook posts because a person allowed to view those posts had provided them to her employer.[66] And in *Sumien v. CareFlite*, the Texas Court of Appeals refused to recognize a right of privacy in Facebook posts viewed by a friend-of-a-friend.[67]

In light of ever-developing technologies that provide ubiquitous tracking and data collection, perhaps, as Justice Sotomayor intimated, it is time to reexamine the public/private dichotomy and third-party doctrine. This reexamination is currently taking place in Fourth Amendment cases, and can easily be applied to common law privacy.

B. "Public" Data and the Mosaic Theory

In 2001, Solove identified the risk to privacy imposed by data analytics: "It is ever more possible to create an electronic collage that covers much of a person's life—a life captured in records, a digital biography composed in the collective computer networks of the world."[68] Tavani succinctly summarizes the fundamental conundrum between data mining (and implicitly predictive analytics) and privacy:

> Unlike personal data that reside in explicit records in databases, information acquired about persons via data mining is often derived from implicit patterns in the data. The patterns can suggest "new" facts, relationships, or associations about a person, placing that person in a "newly discovered" category or group. Also, because most personal data collected and used in data mining applications is considered neither confidential nor intimate in nature, there is a tendency to presume that such data must by default be *public* data. And unlike the personal data that are often exchanged between or across two or more databases in traditional database retrieval processes, in the data mining process personal data are often manipulated within a single database, and typically within a large *data warehouse*.[69]

Derived from government surveillance cases,[70] the "mosaic" theory recognizes that continual surveillance of a suspect's public movements "reveals far more than the individual movements [the whole] comprises."[71] The current leading Fourth Amendment case espousing the mosaic theory is *United States v. Maynard*, in which law enforcement agents tracked a suspect continuously for a month using a GPS device attached to his car.[72] The D.C. Circuit Court of Appeals concluded that the GPS tracking constituted a search within the meaning of the Fourth Amendment and therefore required a warrant.[73] While the U.S. Supreme Court affirmed *Maynard*, it did not do so under the mosaic theory—it instead held that the agents needed a warrant because they physically trespassed when they placed the GPS on the suspect's car.[74] However, in his concurrence with the judgment, Justice Alito expressly stated that he would

"analyze the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove."[75] Justice Alito suggested that the majority's "reasoning largely disregards what is really important (the *use* of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor"—the attaching to the bottom of a car the GPS device itself.[76] And as noted earlier, Justice Sotomayor expressed her opinion "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[77]

One distinguishing factor in the "mosaic" cases is the length of surveillance. "Relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[78] Indeed this was one of Justice Scalia's objections to applying the theory—"it remains unexplained why a 4-week investigation is 'surely' too long."[79] This may be an issue within Fourth Amendment jurisprudence, but it should not be in the context of private-party data tracking and analysis—it is now ubiquitous and fundamentally unavoidable.

Within the context of private-party data tracking and analysis, the mosaic theory is less about length than extremity. New York courts in particular have recognized a common law privacy invasion resulting from overly zealous surveillance of "public" conduct. For example, in *Nader v. General Motors Corporation*,[80] in which General Motors had hired private investigators to follow Ralph Nader, a critic of General Motors, and interview his acquaintances, the New York Court of Appeals concluded that surveillance of public activities could rise to the level of an invasion of privacy.[81] "[I]t is manifest that the mere observation of the plaintiff in a public place does not amount to an invasion of his privacy. But, under certain circumstances, surveillance may be so 'overzealous' as to render it actionable."[82] Judge Breitel elaborated: "Although acts performed in 'public', especially if taken singly or in small numbers, may not be confidential, at least arguably a right to privacy may nevertheless be invaded through extensive or exhaustive monitoring and cataloguing of acts *normally disconnected* and anonymous."[83] Similarly, in *Galella v. Onassis*,[84] a photographer who had stalked former First Lady Jacqueline Onassis to such an extent that he could comment "at considerable length on her personality, her shopping tastes and habits, and her preferences for entertainment,"[85] had invaded Onassis's privacy.[86]

The U.S. Supreme Court has expanded the concept that some public information can be private. Recognizing that "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person,"[87] in *Department of Justice v. Reporters Committee for Freedom of the Press*, Justice Stevens focused on "whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information."[88] Recognizing that complete computerized dossiers are now available at one's fingertips,[89] Justice Stevens concluded that the Freedom of Information Act's exemptions from disclosure recognize "the power of compilations to affect personal privacy that outstrips the combined power of the bits of information contained within."[90] Fundamentally, the Supreme Court has "recognized the privacy interest inherent in the nondisclosure of certain information even where the information may have been at one time public."[91]

Extensive data mining and the use of predictive analytics appear to fit squarely within the concerns expressed by advocates of the mosaic theory, as well as those who have expressed

similar concerns regarding data agglomeration. Citizens should not have to fear that personal and intimate details of their lives will be revealed through the collection, storage, and analysis of virtually all of the mundane acts of life. For all practical purposes, it is now impossible to avoid being tracked:

> Experience has shown that it is *possible*, but it's really not easy, and it comes with a lot of sacrifices. And it requires some technical skill. So to that end, it's my concern about the opt-out idea. I don't actually think it's feasible for everyone to do this. I don't think that's the answer. I don't think that's the simple answer to the big data problem: that you can just turn this stuff off, that you cannot do the things that you clearly need to do for your daily life. But I really want to emphasize, I did this [avoiding tracking] as an experiment to see what it would take, to see what these systems were demanding of us that we'd forgotten about, and how it is that they worked. And so I don't expect people to do this. In fact, I wouldn't recommend it.[92]

We should all not be forced into the experimental "dilemma" attempted by Professor Vertesi of completely rejecting all aspects of modern life—from social communications to shopping—to avoid constant commercial surveillance.[93]

IV. CONCLUSION

The threat to privacy is real, so tradeoffs will have to be considered, beginning with data collection standards. Unfortunately, most calls for standards are fairly amorphous.[94] The World Economic Forum has at least made one fairly concrete suggestion: govern the usage of data rather than the data themselves.[95] Meanwhile, Kerr and Earle conclude that "[b]ig data enables a universalizable strategy of preemptive social decisionmaking that renders individuals unable to observe, understand, participate in, or respond to information gathered or assumptions made about them;" in other words, "big data can be used to make important decisions that implicate us without our even knowing it."[96] As such, they argue for a reexamination of privacy and due process values—"namely, that there is wisdom in setting boundaries around the kinds of assumptions that can and cannot be made about people."[97]

Until the courts begin to recognize the threats to privacy by ubiquitous tracking—preferably through a mosaic theory applied to private trackers—everyone faces the risk of anonymous third parties knowing the intimate details of their private lives. Until then, we have almost no choice but to succumb to the tracking.[98]

---

[1] Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968).

[2] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 2 (2014) [hereinafter BIG DATA: SEIZING OPPORTUNITIES], *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[3] CHARLES NYCE, PREDICTIVE ANALYTICS WHITE PAPER 1 (2007), *available at* www.theinstitutes.org/doc/predictivemodelingwhitepaper.pdf; *see also* HERMAN T. TAVANI, ETHICS AND TECHNOLOGY: CONTROVERSIES, QUESTIONS, AND STRATEGIES FOR ETHICAL COMPUTING 151 (3d ed. 2011) (describing data mining as involving "the indirect gathering of personal information through an analysis of implicit patterns discoverable in data"; noting further that "[d]ata mining activities can generate new and sometimes nonobvious classifications or categories").

[4] NYCE, *supra* note 3; CTR. FOR INFO. POLICY RESEARCH, BIG DATA AND ANALYTICS: SEEKING FOUNDATIONS FOR EFFECTIVE PRIVACY GUIDANCE 1 (2013) [hereinafter BIG DATA AND ANALYTICS], *available at* http://www.hunton.com/files/Uploads/Documents/News_files/Big_Data_and_Analytics_February_2013.pdf

("While traditionally analytics has been used to find answers to predetermined questions, its application to big data enables exploration of information to see what knowledge may be derived from it, and to identify connections and relationships that are unexpected or were previously unknowable.").

[5] *See* BIG DATA AND ANALYTICS, *supra* note 4, at 1 (describing big data as "vast stores of information gathered from traditional sources (e.g., public record data, health data, financial and transactional data) and from new collection points (e.g., web data, sensor data, text data, time and location data and data gleaned from social networks")). "Big data is characterized by the variety of its sources, the speed at which it is collected and stored, and its sheer volume." *Id*.; *see also* Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT'L DATA PRIVACY L. 74, 74 (2013) (referring to big data as "novel ways in which organizations, including government and businesses, combine diverse digital datasets and then use statistics and other data mining techniques to extract from them both hidden information and surprising correlations"). Mayer-Schönberger and Cukier, while noting there is no "rigorous" definition of big data, refer to it as "things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more." VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 6 (2013).

[6] *See, e.g.*, *generally* NYCE, *supra* note 3 (discussing the increasing use of analytics in insurance underwriting). *See also* BIG DATA AND ANALYTICS, *supra* note 4, at 1 (noting that analytics can help identify individuals in need of social services, detect fraud, predict the effects of natural disasters, recognize patterns in scientific research, and discover trends in consumer demand).

[7] Metadata are essentially data about data. *See* EXEC. OFFICE OF THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE xi (2014) [hereinafter BIG DATA AND PRIVACY], *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf ("Metadata are ancillary data that describe properties of the data such as the time the data were created, the device on which they were created, or the destination of a message.").

[8] *See* MAYER-SCHÖNBERGER & CUKIER, *supra* note 5, at 83-97; Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 240 (2013); *see also* Ariana Eunjung Cha, *Turning Medical Care Inside Out*, WASH. POST, May 25, 2014, at A1 (describing how "companies and academic research teams are rushing to make ingestible or implantable chips that will help patients track the condition of their bodies in real time and in a level of detail that they have never seen before").

[9] Ian Kerr & Jessica Earle, *Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy*, 66 STAN. L. REV. ONLINE 65, 65-66 (2013), *available at* http://www.stanfordlawreview.org/sites/default/files/online/topics/66_StanLRevOnline_65_KerrEarle.pdf.

[10] *See* Ericka Menchen-Trevino, *Collecting Vertical Trace Data: Big Possibilities and Big Challenges for Multi-Method Research*, 5 POL'Y & INTERNET 328, 328 (2013); *see also* BEN WABER, PEOPLE ANALYTICS 11-12 (2013) (discussing a "sociometer" that incorporates "the critical sensors necessary to understand many aspects of human behavior"); Emily Singer, *Is "Self-Tracking" the Secret to Living Better?*, MIT TECH. REV. (June 9, 2011), http://www.technologyreview.com/view/424252/is-self-tracking-the-secret-to-living-better (reporting on the self-tracking movement which utilizes wireless sensing devices and smartphones to track personal lifestyle data).

[11] Menchen-Trevino, *supra* note 10, at 328-29; *see also* Sandra González-Bailón, *Social Science in the Era of Big Data*, 5 POL'Y & INTERNET 148 (2013) ("[W]hat makes Big Data unique is their higher level of detail and refinement in the quality of observations, not just the number of data points or the amount of memory that their storage takes.").

[12] González-Bailón, *supra* note 11, at 148.

[13] Menchen-Trevino, *supra* note 10, at 329.

[14] *See* González-Bailón, *supra* note 11, at 147-48 (discussing "end of theory" arguments); *see also* MAYER-SCHÖNBERGER & CUKIER, *supra* note 5, at 70 ("In the future, our understanding will be driven more by the abundance of data rather than by hypotheses."); Chris Anderson, *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, WIRED (June 23, 2008), http://www.wired.com/science/discoveries/magazine/16-07/pb_theory (claiming that "faced with massive data, this approach to science—hypothesize, model, test—is becoming obsolete"). "We can throw the numbers into the biggest computing clusters the world has ever seen and let statistical algorithms find patterns where science cannot." *Id.*

[15] González-Bailón, *supra* note 11, at 148.

[16] MAYER-SCHÖNBERGER & CUKIER, *supra* note 5, at 160.

[17] *Id*.

[18] *Id.* at 161.

[19] *See id.* at 159-161. *See also generally* Matthew L. Jensen et al., *Automatic, Multimodal Evaluation of Human Interaction*, 19 GROUP DECISION & NEGOTIATION 367 (2010) (outlining an approach for automatically extracting behavioral indicators from video, audio, and text and exploring the possibility of using those indicators to predict certain human-interpretable judgments); Thomas O. Meservy et al., *Deception Detection Through Automatic, Unobtrusive Analysis of Nonverbal Behavior*, 20 IEEE INTELLIGENT SYS. 36 (2005) (discussing the theory underlying an automated system that can infer deception or truthfulness from a set of features extracted from head and hands movements in a video).

[20] MAYER-SCHÖNBERGER & CUKIER, *supra* note 5, at 161. Mayer-Schönberger and Cukier remind us that numbers are far more fallible than we sometimes think. *Id*. at 163.

[21] *See* Jeremy Ginsberg et al., Letters, *Detecting Influenza Epidemics Using Search Engine Query Data*, 457 NATURE 1012 (2009) (arguing it is possible to use search queries to detect influenza epidemics in areas with a large population of web search users).

[22] *See* Declan Butler, *When Google Got Flu Wrong*, 494 NATURE 155 (2013) (arguing that mining web and social media data for flu-tracking can only compliment, not substitute for, traditional epidemiological surveillance networks).

[23] BIG DATA AND PRIVACY, *supra* note 7, at 25.

[24] *See id.*

[25] *See* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 8-10 (2004).

[26] *See id.* at 19-20 (discussing the practice of bed-sharing primarily due to the lack of beds and for warmth).

[27] *See* STEPHEN MEYER III, THE FIVE DOLLAR DAY: LABOR MANAGEMENT AND SOCIAL CONTROL IN THE FORD MOTOR COMPANY 1908-1921, at 125 (1981); Samuel M. Levin, *Ford Profit Sharing, 1914-1920: I. The Growth of the Plan*, PERSONNEL J. 75, 78 (1927).

[28] SMITH, *supra* note 25, at 76; *see also* Thomas H. O'Connor, *The Right to Privacy in Historical Perspective*, 53 MASS. L. Q. 101, 104-5 (1968) (asserting that, particularly as a result of the Louisiana Purchase, "the solitary isolation of the explorers, the pioneers, and the settlers of the West was so absolute that privacy was assured by the very physical dimensions which circumscribed the frontier").

[29] *See* Commonwealth v. Lovett, 4 Pa. L. J. Rpts. (Clark) 226, 226 (Pa. 1831) (recognizing "eaves-dropping" as an actionable offense in Pennsylvania, though declining to find the defendant guilty because he was hired by a husband to spy on the husband's wife); DAVID J. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY 2 (1978).

[30] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193, 205 (1890).

[31] *Id*. at 195.

[32] *See, e.g.*, Robert E. Mensel, *"Kodakers Lying in Wait": Amateur Photography and the Right to Privacy in New York, 1885-1915*, 43 AM. Q. 24, 25 (1991) (discussing the impact of unprecedented technological change upon the public's psyche).

[33] *See* Warren & Brandeis, *supra* note 30, at 196 ("The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle."); *see also* Mensel, *supra* note 32, at 25 (arguing that "amateur photography played an important role in provoking outrage among editorial commentators, judges, and legislators which eventually helped lead to the recognition of the right to privacy").

[34] Briscoe v. Reader's Digest Ass'n, Inc., 483 P.2d 34, 37 (Cal. 1971). In *Briscoe*, the California Supreme Court considered whether publication of a criminal's past involvement in a crime could constitute an invasion of privacy if the incident was no longer newsworthy. *See id*. at 43. *Briscoe* was overruled by *Gates v. Discovery Commc'ns, Inc.*, 101 P.3d 552 (Cal. 2004), in which the California Supreme Court ruled, under similar facts, that no invasion of privacy could occur when the broadcast in question relied on public records. "[A]n invasion of privacy claim based on allegations of harm caused by a media defendant's publication of facts obtained from public official records of a criminal proceeding is barred by the First Amendment to the United States Constitution." *Id.* at 562.

[35] *See* BIG DATA AND PRIVACY, *supra* note 7, at ix ("The ubiquity of computing and electronic communications technologies has led to the exponential growth of data from both digital and analog sources."); Diane Cardwell, *At Newark Airport, the Lights Are On, and They're Watching You*, N.Y. TIMES, Feb. 18, 2014, at A1 ("Using an array of sensors and eight video cameras around the [Newark Airport] terminal, the light fixtures are part of a new wireless network that collects and feeds data into software that can spot long lines, recognize license plates and even identify suspicious activity, sending alerts to the appropriate staff."); Robert Faturechi, *You're Being Watched;*

Private Firms Are Building License-Plate Photo Databases that Are Available to Police—And Anyone Else Who Wants to Pay, L.A. TIMES (May 18, 2014), at A1 (reporting what the headline describes); Steve Lohr, *Rise of Data from Sensors*, N.Y. TIMES, Jan. 7, 2013, at B6 ("The ubiquity of sensors is new. . . . The sensors make it possible to get data we never had before.") (quoting David B. Yoffie, a technology and competitive strategy expert at Harvard) (internal quotation marks omitted); *see also* Zach Church, *Google's Schmidt: "Global Mind" Offers New Opportunities*, MITNEWS (Nov. 15, 2011), http://web.mit.edu/newsoffice/2011/schmidt-event-1115.html ("Technology is not really about hardware and software any more. . . . It's really about the mining and use of this enormous [volume of] data [in order to] make the world a better place.") (quoting Google CEO Eric Schmidt) (internal quotation marks omitted).

[36] *See* BIG DATA AND PRIVACY, *supra* note 7, at 19.

[37] *Id.* at 21.

[38] *See id.*

[39] *See* Complaint at 2, *In re* Goldenshores Techs., Inc., FTC Docket No. C-4446 (Apr. 9, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140409goldenshorescmpt.pdf. The FTC entered a settlement with Goldenshores Technologies that requires it to delete personal information collected from consumers as well as provide a just-in-time disclosure that fully informs consumers when, how, and why their geolocation information is being collected, used and shared, and requires defendants to obtain consumers' affirmative express consent before doing so. *See* Decision and Order, *In re* Goldenshores Techs., Inc., FTC Docket No. C-4446 (Apr. 9, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf.

[40] *See* BIG DATA AND PRIVACY, *supra* note 7, at 21.

[41] *Id.*

[42] *See, e.g.*, JULIE BRILL, COMPETITION AND CONSUMER PROTECTION: STRANGE BEDFELLOWS OR BEST FRIENDS? 7 (2010), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/competition-and-consumer-protection-strange-bedfellows-or-best-friends/1012abamasternewsletter.pdf ("In recent years, advances in computer technology have made it possible for detailed information about consumers to be stored, sold, shared, aggregated, and used more easily and cheaply than ever, in ways not feasible, or even conceivable, before. These advances in technology have allowed online companies to engage in targeted advertising, a practice that has many important benefits. . . . Yet serious privacy concerns arise when companies can easily collect, combine, and use so much information from consumers.").

[43] *See* Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES MAG., Feb. 19, 2012, at 30, *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[44] Whenever possible, Target assigns each shopper a unique code that tracks every purchase and which is linked to individual demographic information, such as age, marriage status, neighborhood, estimated salary, credit cards used, and Web sites visited. *Id.*

> Target can buy data about your ethnicity, job history, the magazines you read, if you've ever declared bankruptcy or got divorced, the year you bought (or lost) your house, where you went to college, what kinds of topics you talk about online, whether you prefer certain brands of coffee, paper towels, cereal or applesauce, your political leanings, reading habits, charitable giving and the number of cars you own.

Id.

[45] *See id.* Rather than be among the multiple marketers sending materials post-birth, Target wanted to target (pun intended) women in their second trimester, which is when most expectant mothers begin buying all new and different items, such as prenatal vitamins and maternity clothing. *Id.*

[46] *See id.* (relating how an irate father complained to Target that it was encouraging his teenage daughter to get pregnant by sending her coupons for maternity and baby clothes and cribs, only to find out later that his daughter was indeed pregnant). *But see* Tim Harford, *Big Data: Are We Making a Big Mistake?*, FIN. TIMES, Mar. 29, 2014, at 28 (arguing that pregnant women receive pregnancy-related coupons because everyone on Target's mailing list receives such coupons; suggesting further that Target mixes pregnancy-related coupons with other unrelated coupons not to avoid upsetting pregnant women who would receive only pregnancy-related coupons but because the coupons will be sent to women who are not pregnant). *Cf.* Jessica Goldstein, *Meet the Woman Who Did Everything In Her Power to Hide Her Pregnancy from Big Data*, THINKPROGRESS (Apr. 29, 2014, 11:26 AM), http://thinkprogress.org/culture/2014/04/29/3432050/can-you-hide-from-big-data/ (reporting on the efforts of Jane Vertesi, Princeton University Assistant Professor of Sociology, to prevent "big data" from finding out she was pregnant, and who found hiding from "big data" extremely inconvenient and expensive, besides nearly impossible).

[47] *See* BIG DATA AND ANALYTICS, *supra* note 4, at 2 ("[T]he power of analytics, rich data stores and the insights they can yield raise risks to privacy."). "It is one thing to recommend for a customer books, music or movies she might be interested in based on her previous purchases; it is quite another thing to identify when she is pregnant before her closest family knows." Tene & Polonetsky, *supra* note 8, at 253-54 (footnote omitted).
[48] BIG DATA AND ANALYTICS, *supra* note 4, at 2; *see also* Justin Brickell and Vitaly Shmatikov, *The Cost of Privacy: Destruction of Data-Mining Utility in Anonymized Data Publishing*, 2008 ACM KNOWLEDGE DISCOVERY & DATA MINING CONF. 70, 70 ("[E]ven modest privacy gains require almost complete destruction of the data-mining utility"). *See generally* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010) (demonstrating that cross-linking supposedly anonymous data among databases can "de-anonymize" the data).
[49] BIG DATA AND ANALYTICS, *supra* note 4, at 11.
[50] Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 862 (Cal. Ct. App. 2009).
[51] *See id.* at 863 (citing M.G. v. Time Warner, Inc., 107 Cal. Rptr. 2d 504, 511 (Cal. Ct. App. 2001)).
[52] *See id.* (holding that posting information to MySpace opened it to the public at large, even if it was removed a few days later and was seen by only a few people).
[53] W.A. Parent, *Privacy, Morality, and the Law*, 12 PHIL. & PUB. AFF. 269, 271 (1983).
[54] Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 920 (2005).
[55] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
[56] N.O.C., Inc. v. Schaefer, 484 A.2d 729, 732 n.1 (N.J. Super. Ct. Law Div. 1984).
[57] I.C.U. Investigations, Inc. v. Jones, 780 So. 2d 685, 689-90 (Ala. 2000).
[58] Nelson v. Salem State Coll., 845 N.E.2d 338, 346-47 (Mass. 2006).
[59] 343 U.S. 747, 753-54 (1952) ("Petitioner was talking confidentially and indiscreetly with one he trusted, and he was overheard. This was due to aid from a transmitter and receiver, to be sure, but with the same effect on his privacy as if agent Lee had been eavesdropping outside an open window. The use of bifocals, field glasses or the telescope to magnify the object of a witness' vision is not a forbidden search or seizure, even if they focus without his knowledge or consent upon what one supposes to be private indiscretions."). *But cf.* Kyllo v. United States, 533 U.S. 27, 34-35 (2001) (holding that use of thermal imaging technology constituted a Fourth Amendment search).
[60] 425 U.S. 435, 443 (1976) ("[I]nformation revealed to a third-party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."). *Miller*'s holding was limited by the Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697 (1978) (codified as amended at 12 U.S.C. §§ 3401 – 3422 (2012)), by, for example, requiring the Government authority to notify the bank customer of the subpoena or summons served on the financial institution as well as the nature of the law enforcement inquiry to which the subpoena or summons relates.
[61] 442 U.S. 735, 743 (1979) ("Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Regardless of his location [i.e., whether in his home or some other location], petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call."). *But see* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. III, 100 Stat 1848, 1868 (codified as amended at 18 U.S.C. §§ 3121 – 3127 (2012)) (requiring government authorities to obtain a court order prior to recording telephone numbers dialed).
[62] *See, e.g.*, United States v. White, 401 U.S. 745, 790 (1971) (Harlan, J., dissenting) ("The interest *On Lee* fails to protect is the expectation of the ordinary citizen, who has never engaged in illegal conduct in his life, that he may carry on his private discourse freely, openly, and spontaneously without measuring his every word against the connotations it might carry when instantaneously heard by others unknown to him and unfamiliar with his situation or analyzed in a cold, formal record played days, months, or years after the conversation. Interposition of a warrant requirement is designed not to shield 'wrongdoers,' but to secure a measure of privacy and a sense of personal security throughout our society."); *Smith*, 442 U.S. at 750 (Marshall, J., dissenting) ("[U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity [i.e., the telephone], he cannot help but accept the risk of surveillance.").
[63] *See, e.g.*, RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL SECURITY 140 (2006) ("Information privacy does not mean refusing to share information with everyone. . . . One must not confuse solitude with secrecy; they are distinct forms of privacy."); Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122-23 (2002) (arguing that "treating exposure to a limited audience as identical to exposure to the world" fails "to recognize degrees of

privacy in the Fourth Amendment context"; noting for example, that giving a neighbor keys to one's house so the neighbor can water the plants while the owner is away does not grant the neighbor permission to invite friends into the owner's house); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1086-87 (2002) ("The [Supreme] Court's current conception of privacy is as a form of total secrecy. As conceived by the Court, an individual's hidden world should be protected. It has expressed an interest in safeguarding the intimate information that individuals carefully conceal. Privacy is about protecting the skeletons that are meticulously hidden in the closet. Since information maintained by third parties is exposed to others, it is not private, and therefore not protected by the Fourth Amendment. This conception of privacy is not responsive to life in the modern Information Age. . . .").

[64] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564 (2009). Kerr also argues the third-party doctrine provides clarity by focusing on the information's knowable location rather than its unknowable history. *See id.* at 565. For further elaboration and debate regarding Kerr's arguments, see Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199 (2009); Orin S. Kerr, *Defending the Third-Party Doctrine: A Response to Epstein and Murphy*, 24 BERKELEY TECH. L.J. 1229 (2009); Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239 (2009).

[65] United States v. Jones, 132 S. Ct. 945, 957 (Sotomayor, J., concurring).

[66] Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659, 674 (D.N.J. 2013) ("[T]he evidence shows that Defendants were the passive recipients of information that they did not seek out or ask for. Plaintiff voluntarily gave information to her Facebook friend, and her Facebook friend voluntarily gave that information to someone else. This may have been a violation of trust, but it was not a violation of privacy.").

[67] No. 02–12–00039–CV, 2012 WL 2579525, at *3 (Tex. Ct. App. July 5, 2012). *But cf.* Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 561 (S.D.N.Y. 2008) ("There is no sound basis to argue that Fell [plaintiff's former employee], by inadvertently leaving his Hotmail password accessible, was thereby authorizing access to all of his Hotmail e-mails, no less the e-mails in his two other accounts. If he had left a key to his house on the front desk at [Pure Power Boot Camp], one could not reasonably argue that he was giving consent to whoever found the key, to use it to enter his house and rummage through his belongings. And, to take the analogy a step further, had the person rummaging through the belongings in Fell's house found the key to Fell's country house, could that be taken as authorization to search his country house. We think not.").

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

[69] TAVANI, *supra* note 3, at 151.

[70] *See, e.g.*, Halkin v. Helms, 598 F.2d 1, 8 (D.C. Cir. 1978) ("It requires little reflection to understand that the business of foreign intelligence gathering in this age of computer technology is more akin to the construction of a mosaic than it is to the management of a cloak and dagger affair. Thousands of bits and pieces of seemingly innocuous information can be analyzed and fitted into place to reveal with startling clarity how the unseen whole must operate."); *see also* Halperin v. C.I.A., 629 F.2d 144, 150 (D.C. Cir. 1980) ("We must take into account. . . that each individual piece of intelligence information, much like a piece of jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself.")

[71] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd* sub nom. United States v. Jones, 132 S. Ct. 945 (2012); *see also* Smith v. Maryland, 442 U.S. 735, 748 (1979) (Stewart, J., dissenting) (arguing that a list of telephone numbers dialed could "reveal the most intimate details of a person's life"); United States v. Pineda-Moreno, 617 F.3d 1120, 1125 (9th Cir. 2010) (denying petition for rehearing en banc) (Kozinski, C.J., dissenting) ("By tracking and recording the movements of millions of individuals the government can use computers to detect patterns and develop suspicions. It can also learn a great deal about us because where we go says much about who we are. Are Winston and Julia's cell phones together near a hotel a bit too often? Was Syme's OnStar near an STD clinic? Were Jones, Aaronson and Rutherford at that protest outside the White House? The FBI need no longer deploy agents to infiltrate groups it considers subversive; it can figure out where the groups hold meetings and ask the phone company for a list of cell phones near those locations."); *In re* Application of U.S. for an Order Authorizing Release of Historical Cell-Site Info., 736 F. Supp. 2d 578 (E.D.N.Y 2010) (applying *Maynard* to tracking individuals via historic cell phone location data).

[72] *Maynard*, 615 F.3d at 549.

[73] *See id.* at 563 ("Society recognizes [the suspect's] expectation of privacy in his movements over the course of a month as reasonable, and the use of the GPS device to monitor those movements defeated that reasonable

expectation. [P]rolonged GPS monitoring reveals an intimate picture of the subject's life that he expects no one to have . . . .").

[74] *Jones*, 132 S. Ct. at 949, 951 n.3 ("Where, as here, the Government obtains information by physically intruding on a constitutionally protected area, . . . a search [requiring a warrant] has undoubtedly occurred."). Indeed, the majority openly skirted what many commentators and Court observers considering to be the key issue in the case: "It may be that achieving the same result [i.e., continuous surveillance for a 4-week period] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question." *Id.* at 954.

[75] *Id.* at 958 (Alito, J., concurring).

[76] *Id.* at 961. Justice Alito noted that the basis for the Court's holding in *Jones* would be inapplicable once all cars were fitted with GPS devices. *See id.*

[77] *See supra* text accompanying note 65.

[78] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) ("For [most] offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.").

[79] *Id.* at 954.

[80] 255 N.E.2d 765 (N.Y. 1970).

[81] *Id.* at 771 (applying District of Columbia law).

[82] *Id.* (citing Pinkerton Nat'l Detective Agency, Inc. v. Stevens, 132 S.E.2d 119 (Ga. Ct. App. 1963) (holding that allegations that insurer had detective agency constantly shadow woman after she filed personal injury action against the insurer in a manner calculated to frighten her and give her neighbors the impression that she was engaged in some wrongful activity were sufficient for a claim of invasion of privacy)).

[83] *Id.* at 772 (Breitel, J., concurring) (emphasis added). The New York Court of Appeals did rule, though, that the investigators' interviewing Mr. Nader's acquaintances did not violate his privacy. *Id.* at 770. "Information about the plaintiff which was already known to others could hardly be regarded as private to the plaintiff." *Id.*

[84] 353 F. Supp. 196 (S.D.N.Y. 1972), *aff'd* in relevant part, 487 F.2d 986 (2d Cir. 1973).

[85] *Id.* at 228.

[86] *Id.* ("The surveillance, close-shadowing and monitoring were clearly "overzealous" and therefore actionable.") (applying New York law).

[87] Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 763 (1989).

[88] *Id.* at 764 (noting also that "there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information") (applying the federal Freedom of Information Act, Pub. L. No. 89-554, 80 Stat. 383 (1966) (codified as amended at 5 U.S.C. §§ 551 – 559 (2012))).

[89] *Cf.* Kenneth L. Karst, *The Files: Legal Controls over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROBS. 342, 343 (1966).

[90] *Reporters Comm. for Freedom of Press*, 489 U.S. at 765 (applying 5 U.S.C. § 552(b)(c)).

[91] *Id.* at 767; *see also* Whalen v. Roe, 429 U.S. 589, 605 (1977) ("We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files.").

[92] Goldstein, *supra* note 46; *see also* Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273, 273 (2012) ("[A]vertisers use new, relatively unknown technologies to track people, specifically because consumers have not heard of these techniques. Furthermore, these technologies obviate choice mechanisms that consumers exercise.").

[93] *See* Goldstein, *supra* note 46.

[94] *See, e.g.*, BIG DATA: SEIZING OPPORTUNITIES, *supra* note 2, at 59 (recommending, in part, maintaining privacy values); WORLD ECON. FORUM, PERSONAL DATA: THE EMERGENCE OF A NEW ASSET CLASS 32-36 (2011), *available at* http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (recommending world leaders should take steps to: innovate around user-centricity and trust; define global principles for using and sharing personal data; strengthen the dialog between regulators and the private sector; focus on interoperability and open standards; and continually share knowledge).

[95] WORLD ECON. FORUM, UNLOCKING THE VALUE OF PERSONAL DATA: FROM COLLECTION TO USAGE 4 (2013), *available at* http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf.

[96] Kerr & Earle, *supra* note 9, at 71.

[97] *Id*. at 66.
[98] *See generally* Goldstein, *supra* note 46; *supra* text accompanying note 92.