INFORMATION OVERLOAD: WHY OMNIPRESENT TECHNOLOGY AND THE RISE OF BIG DATA SHOULDN'T SPELL THE END FOR PRIVACY AS WE KNOW IT♦

INTRODUCTION

In March of 2012, the American retail giant Walmart purchased Social Calendar, a Facebook application that provides users with birthday and holiday reminders by e-mail and text message, allows them to send personalized cards and greetings, and provides them with other event planning and scheduling functions.[1] At first blush, this would appear an odd pairing—a company best known as a chain of brick and mortar big-box stores, and an application that exists only within the confines of a separately owned for-profit website. However, prior to its acquisition of Social Calendar, Walmart's purchase of a number of other technology companies revealed a clear effort on the part of the company to improve its e-commerce business.[2]

At that time, Walmart had just launched ShopyCat, a Facebook application of its own that functioned as a gift-recommendation service and portal to Walmart's online store.[3] But if Walmart had its own social

[1] See Sean Gallagher, Walmart Buys a Facebook-based Calendar App to Get a Look at Customers' Dates, ARS TECHNICA (Mar. 16, 2012, 3:15 PM), http://arstechnica.com/business/2012/03/wal-mart-buys-a-facebook-app-to-get-a-look-at-customers-calendars

[2] Leena Rao, *Walmart Buys Facebook's Birthday And Holiday Reminder App Social Calendar*, TECH CRUNCH (Mar. 11, 2012), http://techcrunch.com/2012/03/11/walmart-buys-facebook-birthday-and-holiday-reminder-app-social-calendar.

[3] Id.

media presence that was custom tailored to its business model, what purpose would be served by buying someone else's application rather than simply building its own? The answer is likely that Walmart did not particularly covet the application itself, but rather was after something that it could not easily build on its own: Social Calendar's massive trove of user data, which included 110 million birthdays and other events, the personal information of fifteen million registered users, the usage information of 400 thousand monthly users, and the connections between users.[4] As a result of the acquisition, those users who had provided their information for the purpose of getting updates about their friends' birthdays now face the prospect of a publicly-held company having access to their personal information, and having the ability to do with that information whatever best serves its corporate and shareholder interests.

As Walmart's purchase of Social Calendar suggests, the rapid development of information technology in the twentieth and early twenty-first centuries has had a massive impact on most people's daily lives, especially in regard to personal communications, access to information, and information transport and storage. As a result of these changes, the ability of individuals to control access to their personal information has dwindled, and increasingly, private companies have the freedom, capability, and incentive to collect, analyze, and sell consumer information like never before. While both the Supreme Court and Congress have responded to specific new technologies that have either entered into widespread use or have had particularly significant implications for clearly established rights (for example, technologies with the potential to alter the landscape of law enforcement),[5] there has been little recognition that such pervasive digital technology represents a change not merely in degree, but in kind. Simply put, this development must be addressed in a more comprehensive way. Moving forward under the current legal framework, the omnipresence of advanced information technology threatens to render the Fourth Amendment's protection of personal communications either illusory or obsolete.[6]

---

[4] Id.

[5] *See, e.g.*, Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) ("[E]lectronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment . . . ."); Kyllo v. United States, 533 U.S. 27, 34 (2001) ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use.") (citations omitted); Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2011) (addressing the disclosure of electronic communications and records by internet service providers).

[6] *See* Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1329 (2012) ("Perhaps the Fourth Amendment will fade into the dustbin of history . . . as another idea

In *U.S. v. Jones*, Justices Sotomayor and Alito each authored a concurrence that suggested personal uneasiness regarding attempts to shoehorn modern technology into older legal frameworks such as the third-party doctrine.[7] Justice Sotomayor, in particular, seemed to express an openness to overturning precedent that she considers fundamentally out of step with a more contemporary view of privacy.[8]

In light of these developments, this Note explores the issue of the fading protection offered by the Fourth Amendment as applied to modern communication and digital information. Part I looks at the particular technological changes that appear likely to have a profound and lasting effect on contemporary life; Part II addresses Fourth Amendment jurisprudence, focusing on the third-party doctrine; Part III examines current statutory schemes in the United States and abroad; and Part IV analyzes societal views on information privacy, with attention to the divergence between the average citizen's expectations of privacy and the actual protections offered under the current legal framework.

I. TECHNOLOGICAL DEVELOPMENTS

Computers and information technology have evolved over roughly the past forty years from a mere curiosity, available to and of use to only a select few, to a major global economic force.[9] Within the same period, cellular phones that were once unaffordable and impractical status symbols[10] have become the primary means of telephonic

that galvanized the founding generation but one that speaks to outmoded fears and superseded values. Future courts might reason that as privacy fades, because the citizenry forfeits more and more sensitive information to the private sphere, it takes with it the need for this particular constitutional protection.").

[7] United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) ("Nonetheless, as Justice Alito notes, physical intrusion is now unnecessary to many forms of surveillance. With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones. In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance.") (citations omitted); *id.* at 957 (Alito, J., concurring) ("This case requires us to apply the Fourth Amendment's prohibition of unreasonable searches and seizures to a 21st-century surveillance technique, the use of a Global Positioning System (GPS) device to monitor a vehicle's movements for an extended period of time. Ironically, the Court has chosen to decide this case based on 18th-century tort law.").

[8] *Id.* (Sotomayor, J., concurring) ("More fundamentally, it 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.") (citations omitted).

[9] *See Apple Usurps Google as World's Most Valuable Brand*, REUTERS (May 9, 2011, 2:03 PM), http://www.reuters.com/article/2011/05/09/us-apple-brand-idUSTRE74800D20110509 ("Of the top 10 brands in Monday's report [from global brands agency Millward Brown], six were technology and telecoms companies: Google at number two, IBM at number three, Microsoft at number five, AT&T at number seven and China Mobile at number nine.").

[10] *See* Elwin Green, *After Just 25 Years, Cell Phones Own Us*, PITTSBURGH POST-GAZETTE (Oct.

communication, taking the place of the landline for a significant segment of the population.[11] More recently, the advent of smartphones has shifted the technological landscape: in addition to sending and receiving calls, phones are now comprehensive communications and computing devices used for browsing the Internet, sending text messages, communicating via social media, and navigating by Global Positioning System ("GPS").[12] Coinciding with these recent developments, and perhaps the driving force behind them, has been the explosion in the popularity and utility of the Internet, which continues to play an increasingly dominant role in contemporary life.[13]

While the magnitude of the change wrought by these technologies is widely acknowledged, a clear understanding of its privacy implications is not so widely shared.[14] In many ways, the speed with which technology evolved has led to adoption without comprehension; in professional, educational, and social realms, people are increasingly expected to be competent computer users, regardless of whether they have ever had any in-depth training in or an understanding of the inner workings of these systems. Failure to have at least a working

13, 2008, 12:00 AM), http://www.post-gazette.com/stories/business/technology/after-just-25-years-cell-phones-own-us-414487 ("The first cell phone to market, the Motorola DynaTAC 8000x, weighed 28 ounces (thus its nickname, 'the brick') and had a retail price of $3,995. . . . [I]n his 1987 film 'Wall Street,' Oliver Stone illustrated corporate raider Gordon Gekko's wealth, freedom and power with a scene in which Gekko stands on a beach, phone in hand . . . .").

[11] See, e.g., Stephen J. Blumberg & Julian V. Luke, Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July–December 2009, NAT'L CENTER FOR HEALTH STATS. 1 (May 12, 2010), http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201005.pdf. ("Preliminary results from the July–December 2009 National Health Interview Survey (NHIS) indicate that the number of American homes with only wireless telephones continues to grow. One of every four American homes (24.5%) had only wireless telephones (also known as cellular telephones, cell phones, or mobile phones) during the last half of 2009—an increase of 1.8 percentage points since the first half of 2009. In addition, one of every seven American homes (14.9%) had a landline yet received all or almost all calls on wireless telephones. This report presents the most up-to-date estimates available from the federal government concerning the size and characteristics of these populations.").

[12] For a precise definition of GPS and a description of how it functions, see *Systems, GPS Overview*, GPS.GOV (Jan. 17, 2013) http://www.gps.gov/systems/gps.

[13] *See Computer and Internet Use, About Computer and Internet Use*, U.S. CENSUS BUREAU, http://www.census.gov/hhes/computer/about (last updated May 22, 2012) ("In recent decades, computer usage and Internet access has become increasingly important for gathering information, looking for jobs, and participation in a changing world economy. For those who have both the means and the desire to be connected to the World Wide Web, having computers, laptops, smart mobile phones, or other devices to access the Internet are a necessity.").

[14] *See, e.g.*, Jennifer M. Urban, Chris Jay Hoofnagle & Su Li, *Mobile Phones and Privacy* 24 (Univ. of Cal., Berkeley, Public Law Research Paper No. 2103405, 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405 ("The overall picture we developed from responses to this survey suggests that Americans both use a wide variety of mobile phone features and services that collect a rich set of personal information, and assign a strong privacy interest to that information."); *see generally* Chris Jay Hoofnagle & Jennifer King, What Californians Understand about Privacy Online (Sept. 3, 2008) (unpublished research paper), *available at* http://ssrn.com/abstract=1262130 (concluding that surveyed Californians have a poor understanding of privacy policies and default rules online).

knowledge of these technologies can have severe economic (and increasingly, social) consequences, and thus what may initially appear to be a choice of whether or not to take advantage of the convenience of modern technology is more realistically an ultimatum: keep up, or risk becoming an anachronism.

One result of framing technological engagement as voluntary rather than necessary is that when users disclose personal information in the course of normal online activity, that too is viewed as a voluntary disclosure, even when users are completely unaware that any information exchange is occurring.[15] For example, third-party "cookies"[16]—or "tracking cookies"—allow major marketing and advertising companies to, in essence, tag a computer so that as a user navigates the Internet, her identity can be recognized and her activity can be associated with her identity.[17] As a result, the third-party advertising content provider that surreptitiously plants a cookie is able to assemble a profile of a user's interests based on what she reads, clicks on, and purchases, without ever having to get her affirmative consent.[18]

In addition to the personal information that users unknowingly but "voluntarily" give up as they go about their business online, users also "opt" to give up data that they perceive to be private, but that is actually unprotected by either the law or the applicable privacy policy.[19] This type of information sharing has become increasingly common as social networks have grown in popularity, as they continually encourage users to share a great deal of highly personal information while providing "privacy settings" that give the illusion of control, but in fact provide no legal protection.[20] Likewise, with the increased popularity of "cloud-

[15] Surveys have repeatedly shown that users are opposed to online tracking, even as they remain misinformed about the lack of current protections. *See* Chris Jay Hoofnagle, Jennifer M. Urban & Su Li, *Privacy and Modern Advertising: Most U.S. Internet Users Want 'Do Not Track' to Stop Collection of Data About Their Online Activities* 1–2 (Oct. 8, 2012) (unpublished research paper), *available at* http://ssrn.com/abstract=2152135 ("In previous studies, we have found that Americans think they are protected by strong online privacy laws. Here, we probed beliefs about tracking on medical websites and 'free' websites, with most not able to answer true/false questions correctly about tracking.").

[16] "Cookies are simply text files sent by a Web site to your computer to track your movements within its pages." *See* Adam L. Penenberg, *Cookie Monsters: The Innocuous Text Files That Web Users Love to Hate*, SLATE (Nov. 7, 2005, 4:51 PM), http://www.slate.com/articles/technology/technology/2005/11/cookie_monsters.html. However, while "normal" cookies can only monitor user activity within the host website, third-party cookies are planted by companies that operate across numerous sites on the Internet, and thus can track a much wider range of user activities. *Id.*

[17] Id.

[18] Id.

[19] *See* Hoofnagle & King, *supra* note 14, at 2 ("California consumers overvalue the mere fact that a website has a privacy policy, and assume that websites carrying the label have strong, default rules to protect personal data. In a way, consumers interpret 'privacy policy' as a quality seal that denotes adherence to some set of standards.").

[20] Facebook & Your Privacy, Who Sees the Data You Share on the Biggest Social Network?,

based services," which allow users to upload and store any manner of personal records and documents on third-party servers, but often have terms of service requiring a disclaimer of rights as to the stored documents.[21] Since many of the companies providing these services rely on personalization and customization to differentiate their products and make advertising more targeted, and consequently more profitable, the current system creates incentives to gather as much personal information as possible, rather than to be more transparent or allow users control over how their information is used.[22] The claim that users voluntarily give up this information is belied by companies going to extreme lengths to gather consumer data in ways that could not possibly have been foreseen or consented to by users at the time they initially signed up or disclosed their information. Examples include Google's installation of tracking cookies that bypassed Safari's privacy settings (for which they agreed to pay a fine of almost twenty-three million dollars),[23] Twitter's iPhone application that uploaded and stored all of the e-mail addresses and phone numbers from its users' iPhone contacts lists,[24] or Walmart's purchase of Social Calendar.[25]

In addition to all of the information shared through online activity, recent advances in technology and shifted cultural norms regarding surveillance have allowed for the increased creation and recording of massive amounts of digital information in the "offline" world as well.

CONSUMER REPS. (June 2012), http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm ("Eben Moglen, a Columbia University law professor who supports decentralized data sharing, worries that Facebook's focus on privacy controls is 'like a magician who waves a brightly colored handkerchief in the right hand so that the left hand becomes invisible. From a consumer's viewpoint, Facebook's fatal design error isn't that Johnny can see Billy's data. It's that Facebook has uncontrolled access to everybody's data, regardless of the so-called privacy settings.'").

[21] *See Cloud Computing: Introduction: What is Cloud Computing?*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/cloudcomputing/#introduction (last visited Feb. 21, 2013) ("Under the Electronic Communications Privacy Act, data stored in the cloud may be subject to a lesser standard for law enforcement to gain access to it than if the data were stored on a personal computer. . . . Even where it is clear that user data is protected, cloud computer service providers often limit their liability to the user as a condition of providing the service, leaving users with limited recourse should their data be exposed or lost. . . . [D]epending on the terms of service, deleting an account may not actually remove the stored data from the provider's servers.").

[22] *See* Joseph Menn, *Data Collection Arms Race Feeds Privacy Fears*, REUTERS (Feb. 19, 2012, 2:14 PM), http://www.reuters.com/article/2012/02/19/us-data-collection-idUSTRE81I0AP20120219.

[23] *See* Dara Kerr, *Google Fined $22.5 Million for Safari Tracking*, CBS NEWS (Nov. 19, 2012, 9:03 AM), http://www.cbsnews.com/8301-205_162-57551697/google-fined-$22.5-million-for-safari-tracking.

[24] See David Sarno, Twitter Stores Full iPhone Contact List for 18 Months, After Scan, L.A. TIMES (Feb. 14, 2012), http://articles.latimes.com/2012/feb/14/business/la-fi-tn-twitter-contacts-20120214.

[25] See supra notes 1–4 and accompanying text; see also Aleks Krotoski, Big Data Age Puts Privacy in Question as Information Becomes Currency, GUARDIAN (Apr. 22, 2012), http://www.guardian.co.uk/technology/2012/apr/22/big-data-privacy-information-currency.

Now, seemingly innocuous activities—like carrying a cellular phone,[26] using a customer loyalty card at the store, driving across a bridge, or simply walking around in an urban environment[27]—create trails of information that can later be parsed and analyzed.[28] In the past, as now, these activities and records weren't private, per se, as the activities occurred in public and were subject to observation and recording; however, because observation and record keeping were far from comprehensive, individuals then had the ability to make meaningful decisions about the degree to which they went detected.[29]

Now, constant recording allows surveillance on another level. Where in the past an activity might be observed by a passerby, the passerby's observations were limited by constraints—human hearing, vision, memory, and judgment as to whether an event was notable. These particular limitations allowed for a degree of privacy even for conduct that occurred in public view—one could reasonably determine how much privacy he could expect in light of his surroundings. Where all activity that occurs "in public" is indiscriminately recorded and stored indefinitely, however, those constraints disappear, and suddenly every action is on the record in an entirely different sense.[30] As digital

[26] Op-Ed., *When GPS Tracking Violates Privacy Rights*, N.Y. TIMES (Sept. 22, 2012), http://www.nytimes.com/2012/09/23/opinion/sunday/when-gps-tracking-violates-privacy-rights.html ("The case concerned a drug conviction based on information about the defendant's location that the government acquired from a cellphone he carried on a three-day road trip in a motor home. The data, apparently obtained with a phone company's help, led to a warrantless search of the motor home and the seizure of incriminating evidence.").

[27] Scott Shane, *Data Storage Could Expand Reach of Surveillance*, *The Caucus*, N.Y. TIMES (Aug. 14, 2012, 5:50 PM), http://thecaucus.blogs.nytimes.com/2012/08/14/advances-in-data-storage-have-implications-for-government-surveillance ("Government at every level is experimenting with sophisticated surveillance equipment whose capabilities are improving as rapidly as every other kind of electronic technology. . . . The [New York] Police Department itself, for example, just last week unveiled a new 'domain awareness' system, developed with Microsoft, that links 3,000 cameras, 2,600 radiation detectors and dozens of license plate readers in six locations and mounted on cars. . . . Not so long ago, even the most aggressive government surveillance had to be selective: the cost of data storage was too high and the capacity too low to keep everything. . . . Not anymore. . . . It will soon be technically feasible and affordable to record and store everything that can be recorded about what everyone in a country says or does.").

[28] *Id.* ("The average person today leaves an electronic trail unimaginable 20 years ago—visiting Web sites, sending e-mails and text messages, using credit cards, passing before a proliferating network of public and private video cameras and carrying a cellphone that reports a person's location every minute of the day. . . . And a government sleuth would, of course, be able to efficiently find anything of interest in the data because of the parallel revolution in search technology.").

[29] See Susan W. Brenner & Leo L. Clarke, Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data, 14 J.L. & POL'Y 211, 223-24 (2006) ("Most 'old century' folks may think that their communications and activities are private only insofar as they shield them from observation by others. Such a view tends to associate 'privacy' with enclaves such as our homes, our cars and our offices. . . . [However,] [t]he notion of "private enclaves" as places separate and apart from the world, areas in which our activities and communications are not subject to observation, is disappearing.").

[30] Two extreme examples of this change can be seen in the rapid adoption of facial recognition software, which if cross-referenced against tagged social network photo databases, would serve to

sensors and recording devices grow increasingly pervasive, the ability of an individual to go "undetected" is fading fast.[31]

An important factor in this change has been the drop in the price of information technology and information storage. In the recent past, information storage consisted largely of paper records placed in filing cabinets, a system that would require a massive amount of physical space—not to mention climate control to ensure preservation of the records, and a workforce to file, retrieve, and analyze data—if it were to capture the entirety of the personal information available for about every United States resident. Because of the physical constraints, the creation of a comprehensive paper database of personal information would be cost-prohibitive for even the largest and most ambitious data collector. However, now that networks allow for remote access to digital databases, and an individual's entire cache of personal data can be stored on a single portable hard drive with room to spare, the barriers to massive information storage are dissolving, and indefinite storage of information is fast becoming a reality.[32] Since information can now be

effectively eliminate anonymity in public, and similarly, the adoption of "suspicious behavior"-detecting software, which is programmed to "notice" certain movements that are deemed to presage criminal activity. *See* Michael Kelley, *The FBI's Nationwide Facial Recognition System Ends Anonymity as We Know It*, BUS. INSIDER (Sept. 10, 2012, 4:35 PM), http://www.businessinsider.com/the-fbis-nationwide-facial-recognition-system-2012-9 ("The FBI has begun installing state-of-the-art facial recognition technology across the country as part of an update to the national fingerprint database, Sara Reardon of the New Scientist reports. . . . Reardon notes that the best commercial algorithms can identify someone in a pool of 1.6 million mugshots about 92 percent of the time, even if they aren't looking at the camera."); Dan Jovic, *High-Tech Cameras Watch for Suspicious Behavior at RNC*, FOX 8 CLEVELAND (Aug. 23, 2012, 4:29 PM), http://fox8.com/2012/08/23/high-tech-cameras-watch-for-suspicious-behavior-at-rnc (last visited Mar. 11, 2013) ("The video analyzes the movement with this specialized computer software and it gives them alarms when certain activities occur as body movement and body language.") (internal quotations omitted).

[31] *Hello, Big Brother: Digital Sensors Are Watching Us*, USA TODAY (Jan. 26, 2011, 12:54 AM), http://usatoday30.usatoday.com/tech/news/2011-01-26-digitalsensors26_CV_N.htm ("Several developments have converged to push the monitoring of human activity far beyond what George Orwell imagined. Low-cost digital cameras, motion sensors and biometric readers are proliferating just as the cost of storing digital data is decreasing. The result: the explosion of sensor data collection and storage.").

[32] *See* Shane, *supra* note 27 ("In the 1960s, the National Security Agency used rail cars to store magnetic tapes containing audio recordings and other material that the agency had collected but had never managed to examine, said James Bamford, an author of three books on the agency. In those days, the agency used the I.B.M. 350 disk storage unit, bigger than a full-size refrigerator but with a capacity of 4.4 megabytes of data. Today, some flash drives that are small enough to put on a keychain hold a terabyte of data, about 227,000 times as much."); John Villasenor, *Recording Everything: Digital Storage as an Enabler of Authoritarian Governments*, CENTER FOR TECH. INNOVATION BROOKINGS (Dec. 14, 2011), http://www.brookings.edu/~/media/research/files/papers/2011/12/14%20digital%20storage%20villasenor/1214_digital_storage_villasenor.pdf ("Plummeting digital storage costs will soon make it possible for authoritarian regimes to . . . store the complete set of digital data associated with everyone within their borders. These enormous databases of captured information will create what amounts to a surveillance time machine, enabling state security services to retroactively eavesdrop on people in the months and years before they were designated as surveillance targets.").

stored at a very low cost, companies commonly store more statistical data about their customers than in the past, and increasingly employ various analytics to learn more about customer behavior.[33]

While maintained independently, these records appear fairly harmless; however, issues begin to arise when companies aggregate, process, and mine this information. Where data revealing a consumer's purchases at a particular store might not be particularly telling, combining that information with other databases and outside information can often paint a very detailed picture of an individual. Even where the raw data seems completely innocuous, by searching for patterns within or across data sets, analysts can often reach surprising, non-trivial conclusions about individual preferences, traits, and predilections.[34] Perhaps the most well-known example of sensitive information being gleaned from a seemingly benign data sets was America Online's ("AOL's") release of twenty million web search queries, collected from 650,000 users over a period of three months.[35] While AOL replaced users' names with "user numbers" and removed IP addresses[36] in order to protect their identities, by looking at all of the

[33] *See, e.g.*, Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html ("Whenever possible, Target assigns each shopper a unique code . . . that keeps tabs on everything they buy. 'If you use a credit card or a coupon, or fill out a survey, or mail in a refund, or call the customer help line, or open an e-mail we've [Target] sent you or visit our Web site, we'll record it and link it to your Guest ID' . . . .").

[34] For example, the discount retailing chain Target was able to use sales data to determine which of its female customers were pregnant, as well as how far along they were in the pregnancy. *Id.* ("As Pole's computers crawled through the data, he was able to identify about 25 products that, when analyzed together, allowed him to assign each shopper a 'pregnancy prediction' score. More important, he could also estimate her due date to within a small window, so Target could send coupons timed to very specific stages of her pregnancy. . . . Pole applied his program to every regular female shopper in Target's national database and soon had a list of tens of thousands of women who were most likely pregnant. If they could entice those women or their husbands to visit Target and buy baby-related products, the company's cue-routine-reward calculators could kick in and start pushing them to buy groceries, bathing suits, toys and clothing, as well."). Another striking example of information that can be gleaned from seemingly harmless information occurred in 2009, when M.I.T. researchers created a program that was able to predict male sexual orientation by analyzing Facebook friend networks. *See* Carter Jernigan & Behram F.T. Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation*, FIRST MONDAY (Oct. 5, 2009), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2611/2302. One final example with potentially large-scale political implications is Brian Lapping's PAX Proposal, which seeks to gather information from various sources including news organizations, social networks, mobile phones, and computers, and analyze that information using a predictive algorithm with the goal of identifying areas of political instability and with potential for uprisings. Google has been involved in the preliminary stages of the project, which as of January 2012 was preparing a pilot program. *See* PAX, http://www.paxreports.org/index.php (last visited Feb. 21, 2013).

[35] Michael Arrington, *AOL Proudly Releases Massive Amounts of Private Data*, TECH CRUNCH (Aug. 6, 2006), http://techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data.

[36] An IP address, or Internet Protocol address, is a unique set of identifying numbers assigned to each device that connects with the Internet. *See Beginner's Guide to Internet Protocol (IP)*

searches from an individual user, some of which contained geographic and demographic information, the *New York Times* was able to establish a profile accurate enough to determine a user's identity.[37] Since that incident, it has become increasingly clear that even where an "anonymized" dataset includes nothing that explicitly identifies the user (not even a randomly assigned user identifier, as was the case with the AOL information), "de-anonymization" can be achieved through aggregation and analysis of multiple datasets.[38]

Because this raw information has become so valuable, data-collection and analysis have expanded beyond commercial entities simply trying to come up with ways to better serve their customers: an entire industry devoted to collection, aggregation, analysis, and sales of consumer data has taken root. "[I]t's as if the ore of our data-driven lives were being mined, refined and sold to the highest bidder, usually without our knowledge—by companies that most people rarely even know exist."[39] Now, for every "American adult, the odds are that [Acxiom Corporation, owner of the world's largest commercial database of consumer information] knows things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on."[40]

Given the powerful economic incentives to increase collection and retention of data, it is unlikely that companies will abandon these programs of their own accord. Since private entities seeking to profit from the practice of private data collection are unlikely to institute significant consumer protections absent serious pressure to do so, we now turn to examine the external constraints imposed by the existing legal framework, and the reasons why those too are insufficient in light of recent technological development.

Addresses, ICANN (Mar. 4, 2011), http://www.icann.org/en/about/learning/beginners-guides/ip-addresses-beginners-guide-04mar11-en.pdf.

[37] Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES (Aug. 9, 2006), http://www.nytimes.com/2006/08/09/technology/09aol.html; *see also* Nate Anderson, *"Anonymized" Data Really Isn't—And Here's Why Not*, ARS TECHNICA (Sept. 8, 2009, 7:25 AM), http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin.

[38] *See id.*; *see also* Bruce Schneier, *Why 'Anonymous' Data Sometimes Isn't*, WIRED (Dec. 13, 2007), http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213; Arvind Narayanan & Vitaly Shmatikov, *De-Anonymizing Social Networks*, U. TEX. AUSTIN, http://www.cs.utexas.edu/~shmat/shmat_oak09.pdf (last visited Feb. 21, 2013); Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality*, 25 J. L. MED. & ETHICS, nos. 2 & 3, at 98–110 (1997), *available at* http://dataprivacylab.org/dataprivacy/projects/law/jlme.pdf.

[39] Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES (June 16, 2012), http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html.

[40] Id.

II. LEGAL BACKGROUND

The Supreme Court's definition of what constitutes a "search" under the Fourth Amendment has developed fitfully over time, especially in the context of records that are not obviously within the Amendment's explicitly protected catalog of "persons, houses, papers, and effects."[41] However, throughout the latter half of the twentieth century, the Court consistently, though with notable exceptions, expanded law enforcement's ability to access communications records without first obtaining warrants.[42]

The poles of the informational privacy debate can be seen as growing out of *Katz v. United States* and *United States v. Miller*, decided just nine years later. In *Katz*, the Court abandoned the reasoning of—and expressly overruled—a line of cases suggesting that the constitutional protection from unreasonable search and seizure provided by the Fourth Amendment could only be triggered by an invasion of a physical space analogous to a trespass[43]—the violation of a so-called "constitutionally protected area."[44] In place of a standard that had focused on the physical, the Court substituted a more flexible two-part analysis: under *Katz*, Fourth Amendment protection can be triggered if first, the party asserting a claim to privacy holds a subjective expectation of privacy, and second, that claim can be seen as objectively reasonable.[45] Indeed, although the surveillance at issue in the case

---

41 U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

42 See Silas J. Wasserstrom, The Incredible Shrinking Fourth Amendment, 21 AM. CRIM. L. REV. 257 (1983–1984).

43 *See* Olmstead v. United States, 277 U.S. 438 (1928) (holding that eavesdropping over a tapped phone line was not a violation of the Fourth Amendment where the tap was located outside of the home), *overruled by Katz*, 389 U.S. 347; Goldman v. United States, 316 U.S. 129 (1942) (holding that the recording of a conversation from the other side of a wall, where there was no intrusion into the room, was not a violation of the Fourth Amendment), *overruled by Katz*, 389 U.S. 347.

44 *Katz*, 389 U.S. at 350–51 ("In the first place, the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area.' . . . [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.") (citations omitted).

45 The two-part test presented in Justice Harlan's concurrence would later became the standard framework through which the Court analyzed Fourth Amendment violations:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.

Id. at 361; *see* United States v. Jones, 132 S. Ct. 945, 950 ("Our later cases have applied the

involved a microphone attached to the outside of a public telephone booth, the Court held that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[46]

While the framework offered in *Katz* provided for a nuanced take on personal privacy with the potential to account for technological changes and shifting societal views, within a decade, the *Miller* Court reconstrued "reasonable expectation of privacy" in such a way as to cabin its impact.[47] While ostensibly applying *Katz*, *Miller* in effect walked back the earlier decision, replacing an actual inquiry into subjective intent with a rigid framework dictating that any disclosure of information to a third party makes an expectation of privacy subjectively and objectively unreasonable.[48]

In *Miller*, the defendant argued that his Fourth Amendment rights were violated by the government's use of a subpoena, rather than a warrant, to compel his bank to disclose financial records, and that therefore the unlawfully disclosed evidence ought to have been suppressed.[49] In the majority opinion, Justice Powell defined "knowingly exposes to the public" very broadly, thereby collapsing the two steps of the *Katz* test into one. In concrete terms, Justice Powell found that where an individual makes information accessible to anyone else, even if it is meant to be used for a specific, limited purpose, that individual "knowingly exposes" it to "the public," and cannot claim Fourth Amendment protection.[50] In so holding, Justice Powell replaced the *Katz* Court's flexible approach with a bright-line rule, as exemplified by his truncation of *Katz*'s core concept: while Justice Powell quotes the passage in *Katz* that declares that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection," he omits the caveat that

analysis of Justice Harlan's concurrence in that case, which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy.'") (citations omitted).

46 Katz, 389 U.S. at 353.

47 *See* Brenner & Clarke, *supra* note 29, at 241–42 ("In *Miller*, the Court clearly misapplied its own precedent. First its focus on a 'constitutionally protected area' ignored *Katz*'s statement that the Fourth Amendment protects '*people and not places*.' [Katz, 389 U.S. at 361.] . . . The question the Court should have addressed was not to whom the records belonged, but whether it is in our society's interest to condition a Consumer's use of the nation's banking system on a waiver of his Fourth Amendment privacy.") (emphasis added) (footnotes omitted).

48 Katz v. United States, 389 U.S. 347 (1967); United States v. Miller, 425 U.S. 435 (1976); *see* Brenner & Clarke, *supra* note 29, at 250 ("Whereas *Miller/Smith ipso facto* deny Fourth Amendment protection simply because the Consumer could foresee the risk of disclosure, *Katz* requires the court to evaluate the facts to determine whether the information remains private under the Fourth Amendment *despite disclosure*.")

49 United States v. Miller, 425 U.S. 435, 436–40 (1976).

50 Id. at 442–44.

followed: "But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[51] Where *Katz* tried to do away with categorical distinctions in favor of a "reasonableness" test, [52] *Miller* did precisely the reverse, sidestepping the "reasonableness" analysis by creating a new categorical framework.

Three years after *Miller*, the Court solidified its new categorical approach in *Smith v. Maryland*, where it held that installation and use of a pen register—a device installed on a phone line that records the numbers dialed to make outgoing calls on that line—did not constitute a search under the Fourth Amendment.[53] The majority reasoned that phone users willingly disclose dialing information to the phone company, thereby assuming the risk that those numbers will be disclosed to police, and making any expectations of privacy for such information objectively "unreasonable."[54] While Justice Blackmun's majority opinion in *Smith* purports to apply the *Katz* test and goes through the machinations of the test in a way that the *Miller* majority failed to do,[55] the decision, like *Miller*, rests on a broad definition of "voluntary disclosure" and a zero-sum view of privacy that mandates that any information disclosed be unprotected.[56]

---

[51] Katz, 389 U.S. at 351.

[52] Interestingly, the only Justices on the Court for both *Katz* and *Miller* were Brennan and Marshall, and both dissented in the latter case. For an example of what the more flexible approach to the *Katz* test would look like in practice, see Justice Brennan's dissent in *Miller*, 425 U.S. at 448–49 ("'It cannot be gainsaid that the customer of a bank expects that the documents, such as checks, which he transmits to the bank in the course of his business operations, will remain private, and that such an expectation is reasonable. The prosecution concedes as much, although it asserts that this expectation is not constitutionally cognizable. . . . A bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes. Thus, we hold petitioner had a reasonable expectation that the bank would maintain the confidentiality of those papers which originated with him in check form and of the bank statements into which a record of those same checks had been transformed pursuant to internal bank practice.'") (Brennan, J., dissenting) (quoting Burrows v. Superior Court, 529 P.2d 590, 593–96 (Cal. 1974)).

[53] 442 U.S. 735 (1979)

[54] *Id.* at 745–46 ("[P]etitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record. In these circumstances, petitioner assumed the risk that the information would be divulged to police. . . . We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.' The installation and use of a pen register, consequently, was not a 'search,' and no warrant was required.").

[55] *Id.* at 740 ("This inquiry, as Mr. Justice Harlan aptly noted in his *Katz* concurrence, normally embraces two discrete questions. The first is whether the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy[]—whether, in the words of the *Katz* majority, the individual has shown that he seeks to preserve [something] as private. The second question is whether the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable[]—whether, in the words of the *Katz* majority, the individual's expectation, viewed objectively, is justifiable under the circumstances.") (citations omitted) (internal quotations omitted).

[56] Justice Marshall, in dissent, made precisely this point:

> But even assuming, as I do not, that individuals "typically know" that a phone company monitors calls for internal reasons, it does not follow that they expect this

In *Kyllo v. United States*, the Court again grappled with the standard for Fourth Amendment privacy rights, this time in the context of police use of thermal-imaging cameras to ascertain the temperature of a given spot on the outside of a house.[57] While the case involved direct police surveillance and thus there was no need to address third-party doctrine[58] directly, the decision is noteworthy, both for its analysis of the impact of technology on the Fourth Amendment and for the majority's decision to rely on concepts from *Katz* rather than employ the reasoning of *Miller* and *Smith*.

While Scalia's majority decision in *Kyllo* rests largely on the privileged historical position of the home as a protected private refuge, it also discusses the protection of expectations of privacy, and does not adopt Justice Stevens' "risk assumption" rationale.[59] Justice Stevens, in dissent, argued that there was no legitimate expectation of privacy because the temperature "information" was, in a sense, voluntarily disclosed in that it was released in such a way as to make it "discernible in the public domain."[60] Justice Stevens also argued that the thermal device did not capture the "content" of any communications, and analogized its use to that of a pen register, as in *Smith*, rather than a

> information to be made available to the public in general or the government in particular. Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.

Id. at 749 (footnote omitted) (citation omitted).

[57] 533 U.S. 27 (2001). Whether the device captured information from the outside of the house or revealed information about its interior was a major point of contention between the majority and dissent. *See* Kyllo v. United States, 533 U.S. 27, 35 n.2 (2001) ("The dissent's repeated assertion that the thermal imaging did not obtain information regarding the interior of the home, is simply inaccurate. A thermal imager reveals the relative heat of various rooms in the home. The dissent may not find that information particularly private or important, but there is no basis for saying it is not information regarding the interior of the home.") (internal cross-references omitted); *id.* at 35 ("The Government maintains, however, that the thermal imaging must be upheld because it detected 'only heat radiating from the external surface of the house.'. . . But just as a thermal imager captures only heat emanating from a house, so also a powerful directional microphone picks up only sound emanating from a house. . . . We rejected such a mechanical interpretation of the Fourth Amendment in *Katz*, where the eavesdropping device picked up only sound waves that reached the exterior of the phone booth.") (citations omitted).

[58] Third-party doctrine is the name given to the line of reasoning that precludes any expectation of privacy for information disclosed to a third party. *See* Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528 (2006) ("[Third-party] doctrine provides that if information is possessed or known by third parties, then, for purposes of the Fourth Amendment, an individual lacks a reasonable expectation of privacy in the information.")

[59] *Id.* at 34 ("While it may be difficult to refine *Katz* when the search of areas such as telephone booths, automobiles, or even the curtilage and uncovered portions of residences are at issue, in the case of the search of the interior of homes—the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment.").

[60] Id. at 49–50.

microphone, as in *Katz*.[61]

While Scalia's opinion evinces some concern over technological innovation winnowing away Fourth Amendment protection in certain areas, his ultimate conclusions on that issue are not particularly clear, and, as pointed out by the dissent, his approach leads to paradoxical outcomes.[62] While on the one hand Scalia points out that "[t]o withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment," on the other, he admits that "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[63] Regardless of the somewhat muddled implications of his decision, Scalia clearly rejects the notion that technological capability alone is determinative when it comes to Fourth Amendment rights, and instead reinforces the idea that at least some expectations of privacy are reasonable and legitimate, even where the information could be considered "willingly disclosed" under *Miller* and *Smith*.

Most recently, in *United States v. Jones*, Scalia again wrote for the majority, and as in *Kyllo* he rested his decision on historical notions of privacy.[64] There, Scalia held that the police placement of a GPS tracking device on a car is an occupation equivalent to trespass, and therefore, when done without a valid warrant, constitutes a search in violation of the property owner's Fourth Amendment rights.[65] In so holding, Scalia found the *Katz* test inapt and unnecessary where the

---

[61] *Id.* at 49–50 ("In *Katz*, the electronic listening device attached to the outside of the phone booth allowed the officers to pick up the content of the conversation inside the booth, making them the functional equivalent of intruders because they gathered information that was otherwise available only to someone inside the private area; it would be as if, in this case, the thermal imager presented a view of the heat-generating activity inside petitioner's home. By contrast, the thermal imager here disclosed only the relative amounts of heat radiating from the house; it would be as if, in *Katz*, the listening device disclosed only the relative volume of sound leaving the booth, which presumably was discernible in the public domain.") (Stevens, J., dissenting).

[62] Namely, that the Fourth Amendment protects against home surveillance by uncommon means, but not common means. Theoretically under this rule, an individual can rely on robust protection where there is only a minor threat of a violation, but where there is a more pervasive threat, the individual is not guaranteed any protection. *See id.* at 47 ("Yet how much use is general public use is not even hinted at by the Court's opinion, which makes the somewhat doubtful assumption that the thermal imager used in this case does not satisfy that criterion. In any event, putting aside its lack of clarity, this criterion is somewhat perverse because it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available.") (Stevens, J., dissenting).

[63] Id. at 33–34.

[64] 132 S. Ct. 945, 949 (2012) ("It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

[65] *Id*. ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'") (footnotes omitted).

government physically interferes with a property right, and revealed, contrary to what many scholars and jurists might have thought, that *Katz* had not superseded this older understanding, but rather supplemented it.[66] Because the decision is rooted in property law concepts, Scalia did not delve much into complex theoretical surveillance scenarios, and instead simply stated that non-invasive monitoring would remain subject to *Katz*.[67] In their concurrences, however, Justices Sotomayor and Alito expressed serious concerns about forthcoming complications in Fourth Amendment jurisprudence as a result of twenty-first-century technological advances.[68] Taken together, these opinions reveal that Justices Sotomayor, Alito, Ginsburg, Breyer, and Kagan—a majority of the Court—feel uneasy about potential government surveillance by way of third-party GPS devices.[69]

---

[66] *See* Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, SUP. CT. REV. 2 (forthcoming 2013) ("Writing for the Court, Justice Scalia agreed with the usual story that the Fourth Amendment search doctrine historically was tied to trespass law. According to Justice Scalia, however, *Katz* had supplemented the earlier inquiry rather than replaced it. *Katz* expanded protections *beyond* trespass, but the old trespass test remained in effect all along. This will come as a surprise to scholars and members of the bar who had reasonably understood *Katz* to be the only game in town. But surprise or not, *Jones* teaches that search doctrine now must be understood as including two distinct parts: The *Katz* test and the trespass test.") (footnotes omitted); *Jones*, 132 S. Ct. at 950 ("[F]or most of our history the *Fourth Amendment* was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates. *Katz* did not repudiate that understanding.") (footnotes omitted).

[67] *Jones*, 132 S. Ct. at 953 ("The concurrence faults our approach for 'present[ing] particularly vexing problems' in cases that do not involve physical contact, such as those that involve the transmission of electronic signals. We entirely fail to understand that point. For unlike the concurrence, which would make *Katz* the *exclusive* test, we do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.") (internal cross-references omitted).

[68] *Id.* at 962 ("The *Katz* expectation-of-privacy test avoids the problems and complications noted above, but it is not without its own difficulties. It involves a degree of circularity, and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks. In addition, the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes.") (Alito, J., concurring) (citations omitted); *Id.* at 957 ("More fundamentally, it 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.") (Sotomayor, J., concurring) (citations omitted).

[69] *Id*. at 962 ("[T]he Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked.") (Alito, J., concurring); *id*. at 955-56 ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility.") (Sotomayor, J., concurring) (citations omitted) (quotation marks omitted).

Indeed, although the facts before the Court arguably raised no issue of third-party devices,[70] those Justices nonetheless went out of their way to acknowledge the possibility that current doctrine fails to adequately account for the recent and ongoing society-wide changes brought about by advances in information technology.[71]

Justice Sotomayor's concurrence, especially, recognizes the disconnect between current doctrine and meaningful Fourth Amendment protection going forward. Her analysis recognizes the impact and implications of pervasive digital technology, both in terms of the specifics of GPS tracking,[72] and in terms of the broader issue of third-party disclosure in a society that is increasingly reliant on electronic communications and commerce.[73] Justice Sotomayor's flatly-stated willingness to reconsider the appropriateness of third-party doctrine[74] and her assertion that disclosure for a limited purpose should not preclude privacy[75] suggest a view that such developments threaten to render current Fourth Amendment jurisprudence obsolete unless the Court takes steps to intervene.

Justice Alito, concurring in the judgment, would simply have applied the *Katz* test, rather than relying on concepts of property law, as Scalia did.[76] Among his criticisms of the majority is the claim that the

---

[70] *See id*. at 954 ("We may have to grapple with these "vexing problems" in some future case where a classic trespassory search is not involved and resort must be had to Katz analysis; but there is no reason for rushing forward to resolve them here.").

[71] *Id.* at 962 ("The *Katz* expectation-of-privacy test avoids the problems and complications noted above, but it is not without its own difficulties. It involves a degree of circularity, and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks. In addition, the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes.") (Alito, J., concurring) (citations omitted); *Id.* at 957 ("More fundamentally, it 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.") (Sotomayor, J., concurring) (citations omitted).

[72] Id. at 955–56.

[73] *Id.* at 957 ("People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the 'tradeoff' of privacy for convenience 'worthwhile,' or come to accept this 'diminution of privacy' as 'inevitable,' and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.") (Sotomayor, J., concurring) (internal cross-references omitted).

[74] *Id.* ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

[75] *Id.* ("But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.").

[76] *Id.* at 957–58 ("By attaching a small GPS device to the underside of the vehicle that respondent

bifurcated test creates confusion for digital surveillance by third-party devices—that where the government doesn't physically violate a defendant's space in the traditional sense, but does access electronic information without permission, it could be viewed either as a trespass at the electron level analyzed under the "trespass theory," or as a situation where no physical encroachment occurred, necessitating *Katz* analysis.[77]

Alito acknowledges that the current state of technology and communications has made available a wealth of personal information that, until recently, would have been impossible to collect,[78] but he takes a more measured view than Justice Sotomayor, urging that perhaps disclosure is voluntary, or if not voluntary, at least grudgingly accepted.[79] As a result, where Justice Sotomayor sees a need for judicial resolution, Justice Alito hopes a legislative solution will present itself, while admitting that to date, neither Congress nor most States have "enacted statutes regulating the use of GPS tracking technology for law enforcement purposes," and professing that "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns *may* be legislative," which hardly forecloses judicial action.[80]

Interestingly, outside the Fourth Amendment context, the Supreme Court has recognized both that the aggregation of digital records can have a profound impact on issues of informational privacy, and that information is not necessarily best viewed through the lens of a strict "public/private" dichotomy. In *Whalen v. Roe*, where the Court held that the State of New York was entitled to maintain a centralized database of the names and addresses of people prescribed certain classes

drove, the law enforcement officers in this case engaged in conduct that might have provided grounds in 1791 for a suit for trespass to chattels. And for this reason, the Court concludes, the installation and use of the GPS device constituted a search. . . . This holding, in my judgment, is unwise. It strains the language of the Fourth Amendment; it has little if any support in current Fourth Amendment case law; and it is highly artificial. I 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.") (footnotes omitted) (internal cross-references omitted).

[77] Id. at 961–62.

[78] *Id.* at 963 ("Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen. . . . Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users . . . .").

[79] *Id.* at 962 ("New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.").

[80] Id. at 964 (emphasis added).

of prescription drugs, it nonetheless took notice of "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[81] In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, which concerned a Freedom of Information Act request for disclosure of a citizen's criminal record (containing only the aggregated information from other publicly available records), the Court rejected "respondents' cramped notion of personal privacy,"[82] holding that "a third party's request for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen's privacy," and "when the request seeks . . . merely records that the Government happens to be storing, the invasion of privacy is 'unwarranted.'"[83] Instead of taking the view that there is no privacy interest in material disclosed to the public, the Court emphasized that "[i]n an organized society, there are few facts that are not at one time or another divulged to another," and that "this attribute of a privacy interest supports the distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole."[84] In other words, there can be an interest in maintaining "practical obscurity"[85]: "[p]lainly 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."[86]

III. STATUTORY BACKGROUND

As demonstrated by the flexible approach of the Court in *Reporters Committee for Freedom of the Press*, where there is an underlying statutory framework, it, and not the Constitution or case law,

---

[81] Whalen v. Roe, 429 U.S. 589, 605 (1977). Justice Brennan, in his concurrence, went even further:

> What is more troubling about this scheme, however, is the central computer storage of the data thus collected. Obviously, as the State argues, collection and storage of data by the State that is in itself legitimate is not rendered unconstitutional simply because new technology makes the State's operations more efficient. However, as the example of the Fourth Amendment shows, the Constitution puts limits not only on the type of information the State may gather, but also on the means it may use to gather it. The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.

Id. at 606–07.

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

[83] Id. at 780.

[84] Id. at 763–64.

[85] Id. at 762.

[86] Id. at 764.

determines the amount of weight the Court gives privacy rights.[87] This Section outlines how the current statutory approach to information privacy in this country fails to adequately fill in the gaps created by rigid Fourth Amendment interpretation, and is instead outdated, full of holes, and confusing to contemporary users.

The United States has to date taken a piecemeal approach to information privacy law, resulting in "[a] patchwork of federal and state laws . . . to protect the privacy of certain personal information" rather than serving as a "comprehensive federal privacy statute that protects personal information held by both the public sector and the private sector."[88] In creating this patchwork, Congress has proceeded on a "sector-by-sector" basis, allowing for a great deal of industry self-regulation in most areas, while enacting specific protections for limited (and seemingly arbitrarily selected) categories of information, including consumer credit reports,[89] electronic communications,[90] federal agency records,[91] education records,[92] bank records,[93] cable subscriber information,[94] video rental records,[95] motor vehicle records,[96] health information,[97] telecommunications subscriber information,[98] children's online information,[99] and customer financial information.[100] In other words, the legal default is that information is unprotected; and since most information falls outside of the covered categories, no additional protections apply.

---

[87] *Id.* at 763 ("The question of the statutory meaning of privacy under the [Freedom of Information Act] is, of course, not the same as the question whether a tort action might lie for invasion of privacy or the question whether an individual's interest in privacy is protected by the Constitution.").

[88] Gina Stevens, Cong. Research Serv., R41756, Privacy Protections for Personal Information Online 7 (2011), *available at* http://www.fas.org/sgp/crs/misc/R41756.pdf.

[89] Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1128 (1970) (codified as amended at 15 U.S.C. §§ 1681–1681u (2012)).

[90] Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2522, 2701–2712, 3121-3127 (2012)).

[91] Privacy Act of 1974, Pub. L. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (2012)).

[92] Family Educational Rights and Privacy Act of 1974. Pub. L. 93-380, title V, Sec. 513, 88 Stat. 571 (codified as amended at 20 U.S.C. § 1232g (2012)).

[93] Right to Financial Privacy Act of 1978, Pub. L. 95-630, title XI, 92 Stat. 3697 (codified as amended at 12 U.S.C. §§ 3401–3422 (2012)).

[94] Cable Communications Policy Act of 1984, Pub. L. 98-549, 98 Stat. 2779 (codified as amended at 47 USC §§ 521–573 (2012)).

[95] Video Privacy Protection Act of 1988, Pub. L. 100-618, 102 Stat. 3195 (codified as amended at 18 U.S.C. § 2710 (2012)).

[96] Driver's Privacy Protection Act of 1994, Pub. L. 103-322, title XXX, 108 Stat. 2099 (codified as amended at 18 U.S.C. §§ 2721–2725)).

[97] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936.

[98] Communications Act of 1934, ch. 652, 48 Stat. 1064 (codified as amended 47 U.S.C. 151–162)).

[99] Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, div. C, title XIII, 112 Stat. 2681-2728 (codified as amended at 15 U.S.C. §§ 6501–6506).

[100] Consumer Financial Protection Act of 2010, Pub. L. 111-203, title X, 124 Stat. 1955.

While this "patchwork" might be perfectly appropriate for creating a versatile information privacy law that allows for the proper balancing of commercial and privacy interests in different situations, it is notable that the European Union has taken a much more comprehensive approach—one that is generally seen as much more pro-consumer and pro-privacy.[101] For example, Article Eight of the European Union Convention on Human Rights recognizes a general "[r]ight to respect for private and family life."[102] In furtherance of clearly cementing this right within the new arena of digital records, and in order to avoid a country-by-country patchwork of conflicting laws across Europe, in 1995 the European Commission issued Data Protection Directive 95/46/EC, which laid out the central elements of a data privacy scheme to be adopted into domestic law by each member state.[103]

The Directive established legal requirements for "data controllers," legal rights of "data subjects," and "supervisory authorities" within each member state that would serve to administer the Directive.[104] In contrast to the United States, where regulation is selectively implemented only in certain sectors, the Directive functions as a guarantee of individual rights, applying across the board. It also provides consumers with a governmental body to appeal to when faced with information privacy concerns.

Whether or not the statutory approach of the United States is inherently problematic, its handling of consumer privacy is widely acknowledged to be flawed.[105] The Stored Communications Act

---

[101] *See, e.g.*, Eric Pfanner, *Guarding a 'Fundamental Right' of Privacy in Europe*, N.Y. TIMES (Nov. 20 2012), http://www.nytimes.com/2012/11/21/technology/guarding-a-fundamental-right-of-privacy-in-europe.html ("But Ms. Falque-Pierrotin [head of France's information privacy agency] said her tough approach was justified by the importance that the French, and Europeans more generally, attach to privacy. 'In Europe, we consider privacy a fundamental right,' she said. 'That doesn't mean it is exclusive of other rights, but economic rights are not superior to privacy.' In the United States, she said, despite signs of a new concern about privacy in the digital age, 'personal data are seen as raw material for business.'").

[102] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221, *available at* http://conventions.coe.int/treaty/en/Treaties/Html/005.htm ("1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.").

[103] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281), 31 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[104] *See generally EU Data Protection Directive*, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/privacy/intl/eu_data_protection_directive.html (last visited Jan. 20, 2013).

[105] *See, e.g.*, Miguel Helft & Claire Cain Miller, *1986 Privacy Law Is Outrun by the Web*, N.Y. TIMES (Jan. 9, 2011), http://www.nytimes.com/2011/01/10/technology/10privacy.html ("Many Internet companies and consumer advocates say the main law governing communication

("SCA"),[106] the section of the Electronic Communications Privacy Act ("ECPA")[107] relevant to e-mail, cloud computing, and information stored on social networks, regulates service providers and government access to electronic communications.[108] However, the SCA is a dense piece of legislation that predates the widespread adoption of e-mail, the boom in cloud computing, and the existence of social networks, all of which fall under its purview.[109] Additionally, the law predates the widespread adoption of cellular phones and GPS, so the legal requirements for obtaining either historic or real time tracking data, either by GPS or cell site data, is far from clear.[110]

The aging statute draws distinctions that can seem odd, arbitrary, and out of step with a contemporary understanding of these systems. For example, the SCA is structured around the distinction between "electronic communication services" ("ECS") and "remote computing services" ("RCS"). Different protections apply depending on whether a service is an ECS, RCS, or neither.[111] In general, contemporary users of the Internet and smartphones do not conceptualize online services as falling into these distinct categories, nor do they even realize that such considerations have a profound effect on the legal protection their personal communications receive. Moreover, even for those who are aware that these differences exist, the issue is further complicated by the fact that "most network service providers are multifunctional. They are legally recognized as providers of ECS in some contexts, providers of

privacy—enacted in 1986, before cellphone and e-mail use was widespread, and before social networking was even conceived—is outdated, affording more protection to letters in a file cabinet than e-mail on a server.").

106 18 U.S.C. §§ 2701–2712 (2011).

107 18 U.S.C. §§ 2510–2522 (2011).

108 See Orin S. Kerr, A User's Guide to the Stored Communications Act—and a Legislator's Guide to Amending It, 72 GEO. WASH. L. REV. 1208, 1212-13 (2004) ("First, the statute creates limits on the government's ability to compel providers to disclose information in their possession about their customers and subscribers. . . . Second, the statute places limits on the ability of ISPs to voluntarily disclose information about their customers and subscribers to the government.").

109 *About the Issue*, DIGITAL DUE PROCESS COALITION, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Jan. 22, 2013) ("Since enactment of ECPA, there have been fundamental changes in communications technology and the way people use it, including - Email . . . Mobile location . . . Cloud computing . . . Social networking . . . .").

110 See generally Stephanie K. Pell & Christopher Soghoian, Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact, 27 BERKELEY TECH. L.J. 117, 121–22 (2012) ("Determining the proper access standard—whether the higher 'probable cause' standard, the lower 18 U.S.C. § 2703(d) order requiring 'specific and articulable facts' that the information sought is 'relevant and material to an ongoing criminal investigation,' or some other 'hybrid' standard—is anything but clear under current law. As various courts struggle to apply the Electronic Communications Privacy Act ('ECPA') and the Fourth Amendment to compelled disclosures of location information, a messy, inconsistent legal landscape has emerged . . . . Indeed, the degree of confusion over the appropriate standard to apply to location information is increasing and has spread across judicial districts.") (emphasis added) (footnotes omitted).

111 See generally Kerr, supra note 108.

RCS in other contexts, and as neither in some contexts as well."[112]

Additionally, a series of other dichotomies dictate the precise operation of the Act in any given situation.[113] Those dichotomies are: whether disclosure of a record is voluntary or compelled;[114] whether the provider offers services "to the public" (meaning either a free or pay service available to anyone who wishes to subscribe) or is operating as a "non-public" entity (a provider that offers services only to users who have a special relationship to the provider, such as an educational institution that provides e-mail accounts to its students);[115] and whether the disclosure is "contents of communication" or "noncontent information."[116] In other words, the secureness of an e-mail message on a third-party server depends on whether or not it has been read by the recipient, how long it has been sitting there, whether the company holding it provides services to the public, and whether it is the service provider or the government who seeks disclosure.[117] Once again, these are distinctions that are simply not taken into account by most e-mail users.

Critics also argue that the SCA provides less protection than exists for files saved directly on an individual's computer, or for letters sent through the mail. As the *Washington Post* Editorial Board put it, "If you left a letter on your desk for 180 days, you wouldn't imagine that the police could then swoop in and read it without your permission, or a judge's. But that's just what law enforcement officers can do with your e-mail."[118] The main issue here is that the SCA requires a search warrant only for communications content of messages that are unopened and stored for less than 180 days—other information not within that category can be obtained using other means, including subpoenas, and court orders, with notice sometimes required.[119] While a court order

112 Id. at 1215.

113 Id. at 1224.

114 *Id.* ("In the former, the provider wishes to disclose records to the government; in the latter, the government seeks information from the provider and uses the law to force the provider to disclose the information.").

115 *Id.* at 1226. ("The distinction is important both for compelled and voluntary disclosure rules. In the case of voluntary disclosure rules, the distinction is critical; the SCA's voluntary disclosure limitations apply only to providers that make services available to the public.").

116 *Id.* at 1228. ("Content information is the communication that a person wishes to share or communicate with another person. In contrast, noncontent information (sometimes referred to as 'envelope' information) is information about the communication that the network uses to deliver and process the content information.").

117 Id. at 1223 tbl. (summarizing the basic rules of the SCA).

118 Editorial Board, Editorial, *Keeping Email Private*, WASH. POST (Nov. 28, 2012) http://www.washingtonpost.com/opinions/keeping-e-mail-private/2012/11/28/8f962436-39a8-11e2-a263-f0ebffed2f15_story.html.

119 Unopened e-mail stored more than 180 days, opened e-mail, and other content being stored or processed can be obtained with a subpoena and notice, a 2703(d) order and notice, or a search warrant; noncontent information can be obtained by a 2703(d) order without notice or a search warrant; basic subscriber information, session logs, and IP addresses can be obtained by subpoena

requirement might appear to guarantee a healthy amount of oversight and process for such searches, the restraining power of § 2703(d) is in reality minimal, as it provides that

> [a] court order for disclosure . . . shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.[120]

By requiring that investigators merely demonstrate reasonable belief that an e-mail might be "relevant and material to an ongoing investigation," legislators essentially handed investigators a blank check—law enforcement determines the scope of an investigation in the first place, so anything can be made "relevant and material" by simply broadening the investigation.[121] Additionally this standard allows for law enforcement to cast a wide net, as it requires no showing that the target of the search is suspected of doing something wrong.

Additionally, while the SCA generally bans voluntary disclosure of communications content by public providers, the "emergency" exceptions found in 2702(b) cloud the issue somewhat.[122] Following the terrorist attacks on September 11, 2011, § 2702(b) was broadened by a series of amendments allowing for voluntary disclosure under exigent circumstances, leading to the current phrasing of § 2702(b)(8), which permits disclosure "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[123] The result of this provision is that the government can effectively "request" information rather than compel disclosure by court order (though recipients of government requests, likely unfamiliar with the specifics of the statute,

without notice, 2703(d) order without notice, or search warrant. *See* Kerr, *supra* note 108, at 1223; 18 U.S.C. § 2703(d).

120 18 U.S.C. § 2703(d) (2006).

121 See Stephanie K. Pell & Christopher Soghoian, Can You See Me Know?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact, 27 BERKELEY TECH. L.J. 117, 152 (2012) ("[T]he scope of a D Order may be appropriate even if it compels disclosure of some unhelpful information, as § 2703(d) is routinely used to compel disclosure of records, only some of which are later determined to be essential to the government's case. For example, if investigators compel location information for every cell phone in the vicinity of a murder scene for a specific period of time, they are likely to obtain irrelevant location information . . . in addition to information about the presence of the murderer or witnesses who might have seen the murderer. Broadening the scope of a request for location information beyond, but in relation to, a known target can advance an investigation strategically.").

122 See Brendan J. Coffman, Using Clean Hands to Justify Unclean Hands: How the Emergency Exception Provision of the SCA Misapplies an Already Controversial Doctrine, 1 N.Y.U. INTELL. PROP. & ENT. LAW LEDGER 48 (2010).

123 Id. at 75 (citing 18 U.S.C. § 2702(b)(8) (2006)).

might fail to grasp the difference between an official request for information and a court order demanding the same). In making this request, if the government claims there is an emergency, the provider is essentially free to disclose, as the government's assertion itself can be sufficient to create a "good faith belief" that there is an emergency.[124] Because disclosure is "voluntary," the government insulates itself from blame if it later turns out that there was no imminent risk of harm. Regardless of whether disclosure was in fact justified, the information will remain admissible in court because its disclosure was not unlawfully compelled.

And while government pressure creates strong incentives for service providers to disclose, the statute further stacks the deck against consumers by eliminating a countervailing restraint on overzealous disclosure: though § 2707(d) provides a civil remedy for "persons aggrieved by any violation of this chapter," it only applies where "conduct constituting the violation is engaged in with a knowing or intentional state of mind."[125] Because the government's claim of emergency almost always supports a provider's good faith belief, and the provider almost never has actual knowledge that the request is for another purpose, purposeful violation of the statute is practically impossible, insulating providers and the government from any serious repercussions. [126]

Google's *Transparency Report for User Data Requests in the United States* provides a sense of the number of government requests and the degree of service provider compliance: the report reveals that from January to June 2012, Google received 7,969 user data requests involving 16,281 users/accounts, and that Google produced some data for ninety percent of the requests.[127]

Criticism of the specific operation of ECPA aside, the fact is that it protects a very finite category of information: electronic communications in transit (which are regulated by the aforementioned Pen Register Act and Wiretap Act), and stored electronic

---

124 See Seth Rosenbloom, Crying Wolf in the Digital Age: Voluntary Disclosure under the Stored Communications Act, 39 COLUM. HUMAN RIGHTS L. REV. 529, 565 ("Providers are not capable of evaluating the dangerousness of most 'emergency' situations without government input. In many cases, the provider's understanding of the 'emergency' will rely entirely on the assertions of the same officials who seek disclosure. . . . Nonetheless, the 'good faith' standard and absence of an imminence requirement effectively immunize providers.")

125 18 U.S.C. § 2707 (2012).

126 *See* Coffman, *supra* note 122, at 86 (citing 18 U.S.C § 2707(a) (2006)).

127 Google defines data requests as "Government requests for disclosure of user data from Google accounts or services," and explains that the requests and users/accounts statistic differ because: "There may be multiple requests that ask for data for the same entity or a single request that specifies one or more entities." *Google Transparency Report: User Data Requests, United States*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/US (last visited Feb. 17, 2013).

communications (regulated by the SCA).[128] As noted above,[129] various other statutes protect other types of information, but there is no comprehensive scheme that allows individuals control over how their information is used, and if information does not fall into a specific category, it remains unprotected.[130] Because unregulated entities are free to sell or share data, data can easily be purchased from various sources, aggregated, and resold or shared—resulting in increasingly complete profiles that are not subject to any particular restrictions. The law protects against disclosures by certain types of organizations, but the information itself is unregulated.

The following example reveals the problem with doing things this way (which is only likely to increase as data proliferates further): the Health Insurance Portability and Accountability Act ("HIPAA") protects privacy by regulating disclosures by health plans, health-care clearinghouses, and health-care providers related to a patient's "past, present, or future physical or mental health or condition. . . . the provision of health care to the individual; or the past, present, or future payment for the provision of health care to an individual."[131] However, third-party firms are free to collect data about, among other things, prescription drug purchases and credit card spending that in some cases can reveal more about an individual's medical history than would their actual medical record.[132] Because companies unrelated to health are not

[128] *See* Kerr, *supra* note 108, at 1231 ("While the SCA protects the privacy of stored Internet communications, the Wiretap Act and the Pen Register statute protect the privacy of Internet communications in transit.").

[129] STEVENS, *supra* note 88 and accompanying text.

[130] Chris Jay Hoofnagle & Jennifer King, *Consumer Information Sharing: Where the Sun Still Don't Shine* 4 (2008) (unpublished working paper), *available at* http://www.law.berkeley.edu/files/sb27report.pdf ("[T]o this day there is no comprehensive statutory framework regulating private-sector information collection. Specific federal and state statutes address particular industries, such as information collection in the banking context, but many industry sectors lack information privacy regulation."); *id.* at 6 ("In reality, businesses may sell personal information unless a specific statute regulates the practice. No privacy laws generally limit the sale of personal information by websites, by charities, magazines, or supermarkets. Some states limit banks' sale of information to third parties, but in most cases, banks may sell the information unless the consumer affirmatively objects.").

[131] *What are the Purpose and Background of the Privacy Rule?*, HIPAA PRIVACY RULE, http://privacyruleandresearch.nih.gov/pr_04.asp (last visited Mar. 6, 2013).

[132] Insurance Data: Very Personal Finance: Marketing Information Offers Insurers Another Way to Analyse Risk, ECONOMIST (June 2, 2012), http://www.economist.com/node/21556263 ("[P]ublicly available data will be increasingly useful in helping insurers distinguish the aerobics enthusiasts from the couch potatoes. . . . [S]oftware is now being developed by technology firms . . . to sift through all the marketing data that might help them identify tomorrow's cancer patients or accident victims. Such information can be bought from marketing firms that aggregate data about individuals from records of things like prescription-drug and other retail sales, product warranties, consumer surveys, magazine subscriptions and, in some cases, credit-card spending. At least two big American life insurers already waive medical exams for some prospective customers partly because marketing data suggest that they have healthy lifestyles . . . ."); see also Letter from Marc Rotenberg, Exec. Dir., Elec. Info. Privacy Ctr., and Chris Jay Hoofnagle, Deputy Counsel, Elec. Info. Privacy Ctr., to Representative Adam Putnam, Chair, House Gov't

covered by the Act, they are free to sell that information to anyone they choose, including health insurance companies or other health-care-related service providers.[133]

For all of the above reasons, moving forward, the United States should look to the more comprehensive European model of privacy as an individual right. The pitfalls of the current system—containing laws that are out-of-date, difficult to adapt, increasingly loophole-ridden, limited in scope, and incomprehensible to those they are meant to protect—cannot simply be fixed with a few minor tweaks. Indeed, the White House recently issued a policy paper that seems to have taken its inspiration, at least in part, from Europe, proposing a "Consumer Privacy Bill of Rights" that echoes many of the primary principles of the European Directive.[134] Specifically, the proposal advocates individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability,[135] all of which echo somewhat the E.U. Directive's "right to know who the data controller is, the recipient of the data and the purpose of the processing; the right to have inaccurate data rectified; a right of recourse in the event of unlawful processing; and the right to withhold permission to use data in some circumstances."[136] While this sounds like a promising step in the right direction, "[o]nly time will tell whether the proposal will be implemented in a way that effectively protects user privacy, and that's where the rubber meets the road."[137] Additionally, the proposal does not speak to reforming ECPA and SCA or to limiting third-party doctrine in any way; so presumably both would remain in effect, continuing to lash concepts of privacy to rigid, categorical frameworks.

Reform Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census, and Representative William Clay, Ranking Member, House Gov't Reform Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census (Mar. 25, 2003), http://epic.org/privacy/profiling/datamining3.25.03.html [hereinafter Letter from Marc Rotenberg] ("Collectors of consumer information are willing to categorize, compile, and sell virtually any tidbit of information. For instance, the Medical Marketing Service sells lists of persons suffering from various ailments. These lists are cross-referenced with information regarding age, educational level, family dwelling size, gender, income, lifestyle, marital status, and presence of children. The list of ailments includes: diabetes, breast cancer, and heart disease.").

133 Letter from Marc Rotenberg, *supra* note 132.

134 Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, WHITE HOUSE (Feb. 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

135 Id. at 47–48.

136 *EU Data Protection Directive*: *Background*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/intl/eu_data_protection_directive.html (last visited Jan. 20, 2013).

137 Marcia Hofmann, *Obama Administration Unveils Promising Consumer Privacy Plan, but the Devil Will Be in the Details*, ELECTRONIC FRONTIER FOUND. (Feb. 23, 2012), https://www.eff.org/deeplinks/2012/02/obama-administration-unveils-promising-consumer-privacy-plan-devil-details.

IV. SOCIETAL PRIVACY NORMS

As covered above, the current law allows a huge amount of personal information about any particular individual to be compiled with relatively little cost and effort, and unless the law adapts to account for recent technological innovations, the protections that do exist will continue to weaken as third parties find new ways to capture and aggregate data. As long as third-party doctrine persists, citizens will have no means of controlling the use and dissemination of their personal information other than to "opt out" of major segments of modern life, and the third-party data trade will ensure further proliferation of personal records and increasingly detailed personal profiles—essentially dossiers on law-abiding American citizens. While this information may continue to be privately held, the lack of restraints on these private-sector entities leave them free to disclose or sell any of that information to the government or other actors. In other words, one byproduct of private data-gathering is the possibility of government surveillance and monitoring of citizens on a previously unimaginable scale, by a means that circumvents the legal restraints on government activity—including probable cause and warrant requirements, and the prohibition on maintaining files on citizens not suspected of crimes—by having private entities do the initial information gathering and analysis.[138]

In the case of information privacy, information asymmetry has created a moral hazard where providers are able to insulate themselves from liability through privacy policies that users either do not read or do not understand, as evidenced by consumers' documented, consistent failure to grasp how their information is used.[139] Indeed, the results of a

[138] See, e.g., Danielle Douglas, Consumer Bureau's Cordray Defends Data Collection Before Senate Hearing, WASH. POST (Apr. 23, 2013), http://articles.washingtonpost.com/2013-04-23/business/38756369_1_consumer-financial-protection-bureau-consumer-watchdog-agency-data ("The Consumer Financial Protection Bureau is buying anonymous data and requesting records from banks on more than 10 million Americans to gain greater insight into consumer behavior and the financial marketplace . . . ."). See also Ryan Singel, Newly Declassified Files Detail Massive FBI Data-Mining Project, WIRED (Sept. 23, 2009, 7:00 AM), http://www.wired.com/threatlevel/2009/09/fbi-nsac ("A fast-growing FBI data-mining system . . . now contains tens of thousands of records from private corporate databases . . . ."), and Christopher Slobogin, Government Data Mining and the Fourth Amendment, 75 U. CHI. L. REV. 317, 320–21 (2008) ("[M]any of these programs rely in whole or in part on private companies . . . to provide their input, which is then analyzed by government officials. Companies . . . can provide the inquirer with . . . basic demographic information, income, net worth, real property holdings, social security number, current and previous addresses, phone numbers and fax numbers, names of neighbors, driver records, license plate and VIN numbers, bankruptcy and debtor filings, employment, business and criminal records, bank account balances and activity, stock purchases, and credit card activity.") (footnotes omitted).

[139] See, e.g., Carlos Jensen, Colin Potts & Christian Jensen, Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior, 63 INT'L. J. HUMAN-COMPUTER STUD. 203, 223 (2005) ("What we found in this study, like others, was that only a minority of subjects read policies with any frequency.") (citation omitted); see also Joseph Turow, Chris Jay Hoofnagle, Deirdre K. Mulligan, Nathaniel Good & Jens Grossklags, The Federal Trade Commission and Consumer

2008 study suggest that users might not be able to read these policies even if they tried: at that time, it was found that it would take forty minutes a day for the average consumer to read every word of the privacy policy of every new site she accessed,[140] a number that has almost certainly increased along with the rise in the amount of time people spend online.[141] All of this is to say that self-regulation through disclosure is an inadequate solution that fails to provide consumers a meaningful opportunity to make informed decisions.

However, even while people tend to overestimate the security of their data, when asked about information privacy and security, the majority of those polled in a 2009 survey expressed strong support for greater privacy protections and increased personal control over information.[142] According to the survey, roughly two thirds of Americans objected to online tracking by advertisers, a number that increased when survey participants were told more about current tracking practices.[143] The study also found that 92% of participants expressed support for a hypothetical law requiring marketing and

Privacy in the Coming Decade, 3 I/S: J. L. & POL'Y FOR INFO. SOC'Y 723, 738–39 (2007–2008), available at http://www.ntia.doc.gov/files/ntia/comments/100402174-0175-01/attachments/FTC_and_privacy.pdf ("EULAs, terms-of-service agreements ('ToS'), and privacy policies present complex legal information. Research shows that notices' complexity hampers users' ability to understand such agreements. . . . [T]he policies' formats, locations on the websites, and legal content severely limit users' ability to make informed decisions based on them.") (footnotes omitted). Debra Cassens Weiss, Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print, A.B.A. J. (Oct. 20, 2010, 7:17 AM), http://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_print ("[Chief Justice] Roberts admitted he doesn't usually read the computer jargon that is a condition of accessing websites . . . . Providing too much information defeats the purpose of disclosure, since no one reads it, he said.").

140 Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 543, 563 (2008) ("[The amount of time it would take to read the policies] is slightly more than half of the estimated 72 minutes a day people spend using the Internet. This exceeds the combined percentage of Internet time devoted to shopping (1.9%) dealing with spam (6.2%) and playing games (13%) in 2005. The estimated time to read privacy policies exceeds the percentage of time online that people currently spend surfing the web (45.3%).") (footnotes omitted).

141 Some companies have made a concerted effort to shorten and clarify their privacy policies, but the actual effect of those changes is difficult to gauge. In 2012, Aleecia M. McDonald, co-author of *The Cost of Reading Privacy Policies*, *id.*, explained: "Since our work, there is solid progress on getting users more useful information by rethinking privacy notices altogether. The Internet has changed over the past four years as well, with more third-party data gathering and more Americans online. If we were updating the study we would need to include the time to read policies from the approximately 120 third-parties that most Americans run across in a year, and multiply by more Americans online. The second big change is a huge surge in mobile Internet use . . . . [R]ight now, the majority of mobile apps do not have privacy policies." Michael Kassner, *Reading Online Privacy Policies Cost Us $781 Billion per Year*, TECHREPUBLIC (May 21, 2012, 7:12 AM), http://www.techrepublic.com/blog/security/reading-online-privacy-policies-cost-us-781-billion-per-year/7910.

142 Stephanie Clifford, *Two-Thirds of Americans Object to Online Tracking*, N.Y. TIMES (Sept. 29, 2009), http://www.nytimes.com/2009/09/30/business/media/30adco.html.

143 Id.

advertising companies to delete all personal information they hold about a user upon consumer request.[144] In 2003, another survey found that 85% of the surveyed adults who go online at home stated that they did not agree to the collection and aggregation of their data across multiple sites for purposes of click-stream advertising, even by a "valued" site.[145] When members of the same test group were presented with the option using a "valued" site for free in exchange for permission to "use personal information about you to make money from advertisers," and paying for the site but not allowing information collection, 54% said that they would rather "give up looking for that content on the web" than exercise either option presented.[146]

A 2008 survey of Californians' views on cell phone tracking also suggested a strong preference for enhanced privacy protections.[147] While 83% of respondents agreed or strongly agreed that "[i]n an emergency, the police should be able to find out where I am by tracking *my* cell phone," when asked about "possible rules and procedures to protect data that reveals the location of others," the respondents tended to support restraints on tracking.[148] When asked if they would favor a law that required the police to notify a phone owner before obtaining her location information from the cell phone company, in the context of determining where an individual was one week ago, 72% of respondents supported or strongly supported the notice requirement.[149] When asked if they would favor a law that required the police to convince a judge that a crime was committed in order to obtain historic location information from the cell phone company, 73% supported or strongly supported such a measure.[150]

Moreover, contrary to the common perception that young people have values different from older generations when it comes to privacy,[151] a 2010 study suggests that, with some exceptions, "large

144 Id.

145 A "valued" site was defined as "the website you like most and use regularly." *See* Joseph Turow, *Americans and Online Privacy: The System is Broken*, ANNENBERG PUB. POL'Y CENTER 21–23 (June 2003), http://www.asc.upenn.edu/usr/jturow/Internet-privacy-report/36-page-turow-version-9.pdf.

146 Id.

147 See generally Jennifer King & Chris Jay Hoofnagle, A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Phone Location Information (2008) (unpublished working paper), available at http://www.law.berkeley.edu/files/gbo_location20072.pdf.

148 Id. at 7–8 (emphasis added).

149 Id. at 8.

150 Id. at 8–9.

151 See, e.g., Kashmir Hill, Zuckerberg's Right: Young People Don't Care (as Much) About Privacy, FORBES (Jan. 10, 2010, 2:11 PM), http://www.forbes.com/sites/kashmirhill/2010/01/10/zuckerbergs-right-young-people-dont-care-as-much-about-privacy. This article asserts that a Pew survey showing that younger people viewed "increased security and surveillance measures" over the period of 2000–2009 as a "change for the better" should be taken to mean that they care less about privacy. Of course, where a vote for surveillance is presented as a vote for security, the

percentages of young adults are in harmony with older Americans when it comes to sensitivity about online privacy and policy suggestions."[152] While "[y]oung adults certainly are different from older adults when it comes to knowledge of privacy law" a major part of that difference is that "[t]hey are more likely to believe that the law protects them both online and off."[153] Simple ignorance "may be an important reason large numbers of them engage with the digital world in a seemingly unconcerned manner," and given social pressure to engage in online activity, and an inclination for risky behavior in general, "multiple forms of help from various quarters of society, including perhaps the regulatory arena," might be necessary "to cope with the complex online currents that aim to contradict their best privacy instincts."[154]

In short, taken together, the empirical evidence suggests that, reasonable or not, people do expect and desire privacy protections that strict application of third-party doctrine rejects. Given the amount of information that is beyond the control of consumers, and the comparative lack of understanding people exhibit about how their information is collected and used, to say that as a rule, people lack any subjective expectation of privacy is inaccurate; to say that as a society we are not prepared to recognize those expectations of privacy as reasonable is to ignore that the majority of people continue to agree that such a belief is reasonable, and reveal a strong preference for increased informational privacy.[155]

CONCLUSION

In light of technology's ubiquity, and given that the capabilities of extensive electronic surveillance, data gathering, and data storage are only going to keep expanding, a new legal framework is necessary in order to provide meaningful constraints on the government's information-gathering and monitoring practices. In the absence of reform, the Fourth Amendment itself will continue to lose potency until

survey is intended merely to gauge general impressions about the prior decade, and no questions specifically address contemporary topics of interest related to privacy, to conclude that the results reveal anything meaningful about young people's views on privacy would be a stretch. See id.

152 Chris Hoofnagle, Jennifer King, Su Li & Joseph Turow, *How Different Are Young Adults from Older Adults When it Comes to Information Privacy Attitudes & Policies?*, 3 (2010) (unpublished working paper), *available at* http://ssrn.com/abstract=1589864.

153 Id. at 20.

154 Id.

155 *See* Turow, *supra* note 145, at 28 ("Possibly because of their ignorance of what happens to their information online and how to control it, adults who use the internet at home agree widely and strongly when presented with solutions that let them know straightforwardly what is going on. They strongly support regulations that force more disclosure from online entities. . . . 95% of adults who use the Internet at home agreed or agreed strongly that they should have the legal right to know everything websites know about them. . . . 86% percent agreed *strongly* . . . . 80% also agreed strongly and an additional 14% simply 'agreed' with the statement . . . that 'websites should be required to ask my permission before sending ads to me.'").

eventually private data collection will provide such comprehensive records that it is rendered effectively meaningless by private-sector workarounds and third-party doctrine. Unless a legitimate effort is made to reform the law, individuals will continue to be held responsible for information security "choices" that in reality are merely a reflection of the society-wide changes that information technology has wrought over the last half-century. As technology continues to progress, the powers that be must contend with the fact that what may have at one time been individual choice is fast becoming mandate, and that the "assumption of risk" rationale is unjustifiable. Although the world has seen a shift in the way it conducts business, communications, and surveillance, to say that as a result of one generation's adoption of new methods and means of communication, all present and future individual rights to information privacy were waived, is beyond reason.

In order to construct a functional framework moving forward, great attention should be placed on reconciling the law with the public view of information privacy that actually exists—citizens should not be subjected to objectionable privacy practices based on a view of the law that is vastly out of step with generally shared societal values. While law enforcement and corporate views should be considered as well, part of the problem with the current framework is that it has almost universally come to serve those interests while keeping the citizenry in the dark. The current practice of deferring to law enforcement and allowing it to dictate what sacrifices must be made in the name of security, rather than determining what limits on law enforcement society feels are appropriate, and focusing on private interests at the expense of individual rights, seems to have materialized and ossified in spite of the fact that there is little statutory or Constitutional basis for such an approach. The law and the Constitution do not grant corporations the unconditional right to collect and sell information about consumers without their knowledge or consent, and likewise, do not grant law enforcement the right to employ the most efficient means of gathering information (but frequently mandate the opposite, that law enforcement employ less efficient means to achieve its goals).

These considerations suggest that transparency, realism, and personal control should be the main focus of efforts to revitalize privacy. First and foremost, statutory rejection of strict third-party doctrine, and an overhaul of e-mail, cloud computing, and cellular location-tracking rules would provide the groundwork, as such changes would realign the law with common conceptions about informational security. Second, a focus on creating enforceable, individual rights, such as those in Europe, would bring economic and social pressures to bear on those groups that currently only have incentives to gather information. If a more realistic, nuanced view of privacy does not take

root, the Fourth Amendment, and privacy in general, will mean nothing more than the right to maintain the secrecy only of one's own innermost, undisclosed thoughts.

*Devin Ness**

* J.D. candidate, Benjamin N. Cardozo School of Law (2014); Senior Articles Editor, Cardozo Arts & Ent. L.J. Vol. 32; B.A., *cum laude*, New York University (2007). I would like to thank the editors of the Cardozo Arts & Entertainment Law Journal for all of their advice, assistance, and hard work. Thank you also to all of my friends and family, especially Mom, Dad, Alexander, and Sally, for their unwavering support and love, and Kristen, for her generosity and encouragement throughout this process.