Spring 2016 www.lawtechjournal.com Volume 20, Issue 1

UCLA Journal of Law & Technology

THE PRICE OF PRIVACY: HOW ACCESS TO DIGITAL PRIVACY IS SLOWLY BECOMING DIVIDED BY CLASS

Michael Rosenberg

The Fourth Amendment's Third Party Doctrine has recently been extended to cover a person's interest in their digital information. This has allowed more data to become accessible to government agencies than ever before. Under this doctrine, as soon as digital information is provided to a third party (such as Google or Facebook), it is no longer entitled to a presumption that the originator of the information deemed it to be "private." As a result, digital information provided to or through a third party is not entitled to Fourth Amendment protection against the State. Private companies have begun pushing back against this unprecedented government access by creating products to make individual communications more secure against both hackers and the government. Those who are able to afford these high-tech security gadgets and encryption technologies are able to enjoy enhanced security over their "private" information. However, those unaware of or unable to afford these products are left with inadequate Fourth Amendment protections for keeping their digital information free from government access. Unfortunately, this has created a discrepancy in the constitutional protections afforded to ordinary citizens based on socioeconomic status: those with money are able to increase the security of their digital information against the state while those with lesser means remain exposed. This article advocates for the acknowledgment of this phenomenon and suggests possible solutions to this disparity.

TABLE OF CONTENTS

The Price of Privacy: How Access to Digital Privacy Is Slowly Becoming Divided by Class

Michael Rosenberg

Introduction

In the realm of digital information, "if you aren't paying for the product, you are the product."[1] In other words, as businesses continue to increase the amount of data they store on individuals, the data itself becomes a product for sale. Unless consumers purchase goods and services to protect themselves from divulging digital information, they run the risk of having their private data bundled and sold for a profit.

Businesses collect an astounding amount of digital information on individuals. In modern society, most people rely on their smartphones, laptops, and tablet devices to interact with people and companies from all over the world. These devices are used during school, work, and play. We use Google to search for a restaurant, use iMessage to text one another about plans for the night, post pictures of our meals to Instagram, and pay for the night using our credit cards. Along the way, each of these companies track every interaction we make online through their hardware and software.[2] They track our likes and dislikes, curiosities, and even locations. Our online presence has become a reflection of our personalities, interests, and identities. Our phones, our computers, and how we use them are no longer just a reflection of our communications between one another – they reflect our entire lives.

By collecting people's digital information, companies can aggregate data to form a comprehensive picture of a person's desires. This information is invaluable as a marketing tool,

---

[1] Julia Angwin, *Has Privacy Become A Luxury Good?*, N.Y. TIMES (Mar. 3, 2014), http://www.nytimes.com/2014/03/04/opinion/has-privacy-become-a-luxury-good.html.

[2] *See* Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1310 (2012); Caitlin Dewey, *Everything Google Knows About You (and How it Knows it),* WASH. POST (Nov. 19, 2014), http://www.washingtonpost.com/news/the-intersect/wp/2014/11/19/everything-google-knows-about-you-and-how-it-knows-it/.

so companies often repackage the data and sell it for a profit.[3] However, businesses are not the only ones that benefit from this collection of private data; the government has been granted access to digital information collected by the private sector. Due to the gradual expansion of the "Third Party Doctrine," the government has been increasingly successful at convincing courts that the collection of a citizen's digital information obtained through a third party, regardless of quantity, does not infringe upon any Fourth Amendment constitutional rights.[4] According to the government, this information has been necessary in solving a wide variety of crimes.[5]

Though it had previously been known that the government would occasionally request a citizen's information pursuant to an ongoing criminal investigation, the true extent of the government's surveillance practices was not revealed until recently. In 2013, National Security Agency contractor Edward J. Snowden leaked documents to the Guardian, the Washington Post, and Germany's Der Spiegel media properties in which he disclosed how the National Security Agency had collected "vast troves of data on smartphone users by back-ending data centers of the carriers themselves."[6] Essentially, Snowden revealed that in the name of national security, the government is collecting at least *all* of a cell phone user's metadata regardless of whether or not that user is a suspect in an ongoing criminal investigation.

Notwithstanding the government's justification for their global surveillance programs, knowledge of their surveillance practices has caused many Americans to become extremely

---

[3] *See, e.g.*, John R. Quain, *Changes to OnStar's Privacy Terms Rile Some Use*rs, N.Y. TIMES (Sept. 22, 2011, 6:00 AM), http://wheels.blogs.nytimes.com/2011/09/22/changes-to-onstars-hprivacy-terms-rile-some-users/ (explaining how OnStar changes some of its privacy terms so as to be able to sell driver data to other companies).

[4] *See, e.g.*, ACLU v. Clapper, 959 F. Supp. 2d. 724 (S.D.N.Y. 2013) (finding the National Security Agency bulk telephony metadata collection program constitutional under the Third Party Doctrine).

[5] James B. Comey, Director, Federal Bureau of Investigation, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, Speech Before the Brookings Institution (Oct. 16, 2014), *accessible at* http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[6] Richard Byrne Reilly, *New Ultra Secure Cell Phone, Blackphone, is Reportedly Flying off the Shelves*, VENTUREBEAT (Sept. 3, 2014, 4:09 PM), http://venturebeat.com/2014/09/03/new-ultra-secure-cell-phone-blackphone-is-reportedly-flying-off-the-shelves/

critical of government oversight.[7] Many fear that the rise of the surveillance society has begun.[8] In response to both the Snowden disclosures and an increasing contention over bulk data collection, a market of products and services that shield an individual's digital information from government oversight has emerged.[9] Companies that previously disclosed information to the government are now competing to garner the best reputation for protecting their users' private information.[10] Some companies have even sprung into existence solely from the increasing market need for privacy-related products.[11]

As a market develops for selling the "peace of mind" that comes with protecting consumers from expansive government surveillance and oversight, we are left wondering what role the protections of the Fourth Amendment play regarding digital information. When searching the marketplace for a product or service that provides protection from surveillance, one must be able to afford the service or have knowledge about how to protect their information in the most cost-effective manner. As such, only those knowledgeable about how to protect their digital information from exposure or those able to afford products that do so can protect themselves from the government's acquisition of their information. Thus, purchasing privacy requires knowledge, power, and wealth. This cost will create a divide between the privacy protections afforded to those belonging to different socioeconomic classes.

---

[7] *See, e.g.*, Comey, *supra* note 5 ("In the wake of the Snowden Disclosures, the prevailing view is that the government is sweeping up all of our communications.").

[8] *See* Ohm, *supra* note 2, at 1312.

[9] Some have predicted that the market may step in to fill the gap in Fourth Amendment protections. *Id.* ("[T]he rise of the surveillance society will break the connection between privacy and liberty from power and will force us to protect the core value of the Fourth Amendment through other means.").

[10] *See* Craig Timberg, *Apple Will No Longer Unlock Most iPhones, iPads for Police, Even With Search Warrants*, WASH. POST (Sept. 18, 2014), http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html ("Apple . . . is making it impossible for the company to turn over data . . . to police . . . taking a hard new line as tech companies attempt to blunt allegations that they have too readily participated in government efforts to collect user information."); Reilly, *supra* note 6 ("There has been a remarkable convergence of market opportunity and timing, Snowden crystalized the awareness of bulk surveillance.").

[11] *See, e.g.*, Reilly, *supra* note 6 (detailing the launch of Blackphone, whose entire selling point is its ability to protect a user's private information from detection).

This paper seeks to explore the emergence of the new market for privacy-protecting goods and services, and how the disparate treatment in privacy protections between the rich and the poor under current Fourth Amendment jurisprudence is exacerbated by the fact that obtaining these goods require knowledge, power, and wealth. Part I will briefly discuss how different social classes have historically been afforded differing levels of constitutionally protected Fourth Amendment rights. Part II will discuss the emergence of these new privacy-protecting products and services, and how they lead to the historical discrepancy of privacy protections across class lines will soon be expanded to also encompass one's interests in their digital information. Part III will discuss why this protection of digital information across class lines is problematic and why all American citizens should be concerned about this disparity of treatment. Finally, Part IV will discuss possible solutions to mitigate the development of this disparity as technology develops further.

I. Fourth Amendment Doctrine Creates A Disparity in Which Those Belonging to Different Social Classes Receive Differing Levels of Constitutional Protection

The Fourth Amendment entails "the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures."[12] Defining what is secure and determining when a search or seizure is unreasonable has proven to be difficult in practice. Courts currently use the "Reasonable Expectation of Privacy" test derived from *Katz v. United States*.[13] According to Justice Harlan's concurrence, an unreasonable search or seizure occurs when it violates a plaintiff's reasonable expectation of privacy.[14] To demonstrate such a violation, a plaintiff must be able to affirmatively prove: (1) that the search violated their subjective sense of privacy (i.e. that the plaintiff felt that they were being private), and (2) that their expectation of privacy was reasonable (i.e. that the plaintiff's expectation of privacy was one in which society is prepared to deem "protected.").[15]

The "Reasonable Expectation of Privacy" test, though helpful to courts, is often difficult to apply across widely varying factual situations. The difficulty arises when determining what standard should be applied to evaluate whether a person's expectation of privacy is objectively

[12] U.S. CONST. amend. IV.
[13] Katz v. U.S., 389 U.S. 347 (1967).
[14] *Id.* at 360 (Harlan, J., concurring).
[15] *Id.* at 361.

reasonable. If the law revolves around what may generally be considered a "reasonable expectation of privacy," then the definition is circular in that the government may condition the citizenry to expect little to no privacy. How, then, should courts objectively determine whether or not an expectation of privacy was reasonable? In response to this quandary, "privacy" has grown to encompass a "positive" definition in which the courts evaluate the privacy expectations that neighbors have among one another to determine the appropriate privacy expectations one has against the police. Therefore, "the kind of privacy protection citizens have vis-à-vis the police is tied to the kind of privacy the same citizens have with one another."[16] In other words, the reasonableness of a person's expectation of privacy is "contingent upon the existence of 'effective' barriers to intrusion."[17] This conceptualization of privacy has proven helpful to the courts since Fourth Amendment law can change people's expectations of privacy from the state but can do little to affect their expectation of privacy from one another.

By tying the privacy expectations that citizens have with the police to the privacy expectations that they have with one another, the "Reasonable Expectation of Privacy" test favors those who can reasonably expect a greater degree of privacy from others. Privacy exists only in certain types of spaces. Thus, people with more money and more power will be able to purchase more privacy protections than those with fewer means. Since rich people have access to more private spaces than poor people, the rich are able to garner greater Fourth Amendment protections. For example, the poor typically live in apartment buildings in congested, urban areas. People may be able to hear sounds or smell cooking from inside an apartment unit when walking down the apartment building's staircase, and possibly even see inside the unit through a window while standing on a nearby street. On the other hand, wealthier people may be able to afford a stand-alone house in the suburbs with a yard, driveway, and ample space between neighboring homes. People would likely be less able to sense anything inside the home from the distant sidewalk or street. Therefore, before the law is even applied, the poor begin with less privacy protections between one another than do the middle-class or the rich.

---

[16] William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1267 (1999).
[17] Christopher Slobogin, *The Poverty Exception to the Fourth Amendment*, 55 FLA. L. REV. 391, 400 (2003).

The theory that those who start out with less privacy between one another also receive fewer Fourth Amendment protections has proven true in practice. In fact, many cases in which this appears involve police using developing technologies to investigate the curtilage of a suspect's home.[18] In *California v. Ciraolo*, police officers learned that the defendant may have been growing marijuana in his backyard and went to the defendant's premises to investigate.[19] When the officers discovered that a ten-foot tall fence enclosed the defendant's yard, they chartered a private plane to view the scene from above.[20] The officers' view from 1,000 feet above the field allowed them to see marijuana plants growing in the defendant's yard.[21] The Supreme Court, despite finding that the defendant's backyard was a part of the curtilage of his home, declared the search reasonable.[22] The court held that since "any member of the public flying in this airspace who glanced down could have seen" the marijuana plants, the defendant knowingly exposed his illegal activity to the public.[23] Because the defendant didn't fully enclose his yard despite constructing his fence, his yard remained exposed from above and was susceptible to constitutional police surveillance.

The Supreme Court delivered a similar holding in *Florida v. Riley*.[24] In *Riley*, the police received a tip that the defendant was growing marijuana in a greenhouse in the backyard of his property.[25] Because the alleged marijuana plants were inside the building, the police were not able to see the plants from outside.[26] The police then chartered a helicopter to fly 400 feet above

---

[18] "Curtilage" is considered to include "portions of a homeowner's property so closely associated with the home as to be considered a part of it," such as a porch, an attached garage, or a detached shed. *See* United States v. Pineda-Moreno, 617 F.3d 1120, 1121 (9th Cir. 2010) (Kozinski, J., dissenting). For a discussion about how police use of technology in areas of curtilage negatively impact the poor, see Amelia L. Diedrich, *Secure in Their Yards? Curtilage, Technology, and the Aggravation of the Poverty Exception to the Fourth Amendment*, 39 HASTINGS CONST. L.Q. 297 (2012).

[19] California v. Ciraolo, 476 U.S. 207, 209 (1986).

[20] *Id.*

[21] *Id.*

[22] *Id.* at 213-214.

[23] *Id.* at 210.

[24] Florida v. Riley, 488 U.S. 445 (1989).

[25] *Id.* at 448.

[26] *Id.*

the defendant's yard and were able to see inside the building through its roof.[27] The court, mirroring the rationale espoused in *Ciraolo*, determined that the officers did not violate the defendant's Fourth Amendment rights.[28] The court explained that the officers merely changed their vantage point to another location in a public space, from which any member of the public could have viewed inside of the defendant's greenhouse.[29] Although the defendant in *Riley* did more than the defendant in *Ciraolo* to enclose his plants inside of a building within the curtilage of his home, the transparent roof of the greenhouse was still not deemed enough of an effective barrier of intrusion to prevent the officers from committing an unreasonable search.

Finally, in *United States v. Pineda-Moreno*, Drug Enforcement Agency agents attached a mobile tracking device to the defendant's vehicle while it was parked in the defendant's driveway.[30] The agents hoped to use the device to catch the defendant traveling to and from a suspected marijuana-growing site.[31] After attaching the device, the agents did in fact observe the defendant leaving the suspected site and pulled him over to find a large quantity of marijuana inside his vehicle.[32] When the defendant tried to appeal the district court's ruling against suppression of the evidence to the Ninth Circuit, the court held that although the defendant's car was located in the curtilage near the home, the defendant had not done enough to establish a reasonable expectation of privacy by "'detailing the special features of the driveway itself (i.e. enclosures, barriers, lack of visibility from the street) . . . .'"[33] Therefore, the defendant maintained no reasonable expectation of privacy in his driveway and did not suffer a violation of his constitutional rights.[34]

---

[27] *Id.*
[28] *Id.* at 449.
[29] *Id.* at 449-50.
[30] United States v. Pineda-Moreno, 591 F.3d 1212, 1213 (9th Cir. 2010), *en banc reh'g denied*, 617 F.3d 1120 (9th Cir. 2010), *cert granted, judgment vacated*, 132 S. Ct. 1553 (2012).
[31] *Id.* at 1213-14.
[32] *Id.* at 1214.
[33] *Id.* at 1215 (quoting Maisano v. Welcher, 940 F.2d 499, 503 (9th Cir. 1991)).
[34] The physical trespass of the attached mobile tracking device upon the defendant's vehicle would now be considered a violation of the Fourth Amendment in light of the Supreme Court's decision in United States v. Jones, 132 S.Ct. 945 (2012). However, the criteria that the defendant be able to demonstrate actions taken to secure his premises, absent a physical trespass by the government, remain intact for purposes of future Fourth Amendment inquiries.

Each of these three cases demonstrate how the court evaluates the privacy expectations that citizens have between one another to draw an analogy to the privacy expectations that members of the public have with the police. The cases also show the significance of how one's privacy in relation to the public could be detrimental to one with few means for protecting such privacy. The defendant in *Ciraolo* had a ten-foot fence around his yard, but that wasn't enough to demonstrate a reasonable expectation of privacy on his land. In order for the defendant to overcome the rationale of the decision in his case, he likely would have needed to build a canopy over his yard or somehow enclose his plants within a structure. This would have required time, energy, and most significantly, money. Depending on the size of the yard, this may not have been feasible. The defendant in *Riley*, on the other hand, did enclose his plants within a structure – the plants were stored inside of a greenhouse on his property. Even this was not enough to establish a reasonable expectation of privacy since the officers could still see inside the building from above. This shows that even when property within the curtilage of the home is concealed on all sides, it must be completely obscured from view. A hole in the roof or a broken window could mean the difference in finding a constitutional violation. Unfortunately, one must have the means to build the concealing structure in the first place or to repair their roof or window immediately in order to feel confident that their constitutional rights will be maintained.

This line of reasoning was especially troublesome to the Chief Judge of the Ninth Circuit Court of Appeals, Judge Kozinski. He wrote a dissent from the denial of rehearing where he criticized the *Pineda-Moreno* court for creating a constitutional standard where poor individuals receive less Fourth Amendment protections than their wealthier counterparts.[35] Kozinski argued that if the standard for the protection of privacy focused upon the amount of privacy an individual has with members of the public at large, then the wealthy will be able to protect and bolster that privacy "with the aid of electric gates, tall fences, security booths, remote cameras, motion sensors, and roving patrols."[36] His fear was that those without the means to protect their privacy from others, in other words those with "open driveways, unenclosed porches, basement doors left unlocked, back doors left ajar, yard gates left unlatched, [and] garage doors that won't

[35] Pineda-Moreno, 617 F.3d at 1121 (Kozinski, J., dissenting).
[36] *Id.*

quite close," will be at an extreme disadvantage in claims against the government.[37] The Chief Judge ultimately stressed his point that "poor people are entitled to privacy, even if they can't afford all the gadgets of the wealthy for ensuring it."[38]

Unfortunately, the current application of Fourth Amendment doctrine tends to favor the wealthy over the poor in a number of situations. To the extent the law remains focused on a reasonable expectation of privacy, some citizens will undoubtedly receive more constitutional protection than others.[39] Traditionally, this disparity in treatment has mostly been confined to Fourth Amendment challenges regarding a person's physical space and possessions. However, with the relatively recent emergence of a market for privacy-protecting goods and services for one's digital information, this disparity has the potential to bleed into one's digital space and possessions as well.

II. The Discrepancy of Fourth Amendment Privacy Across Class Lines Has Expanded Into the Realm of Digital Information

a. The Nature of Communication Between Consumers and Businesses Has Changed Radically Over Recent Decades

The Internet has drastically changed how people communicate and interact with one another. It allows consumers to have constant access to a wealth of information. A consumer can quickly search online to find out the show times of a movie, the phone number of a store, or the distance to a nearby restaurant. Recent technological progress has raised convenience and simplified communications between consumers and businesses. As companies transition towards smaller and lighter hardware with more advanced and capable software, Internet consumption has never been greater. The rise of consumption, however, has led at least one scholar, and likely others, to fear the rise of the "Surveillance Society."[40] Three major technological developments – social networks, cloud computing, and smartphones – have contributed the most to the increase of digital information output and the propulsion of these fears.

---

[37] *Id.*
[38] *Id.* at 1123.
[39] For a brief discussion about a positive definition of privacy as opposed to a normative definition, see Stuntz, *supra* note 16, at 1267, 1272.
[40] *See* Ohm, *supra* note 2, at 1310.

Social networking platforms allow people to communicate with one another and express themselves online. Some networking sites such as Facebook, Google+, and Twitter are used for casual interaction, while other networking sites such as LinkedIn are used for professional interaction. A consumer may use Instagram to share a picture that has a fancy filter, but if the consumer wants the photo to "disappear" within a few seconds, the consumer may share it via Snapchat instead. Furthermore, an increasing number of games are becoming social networking platforms because they involve an element of cooperation and interaction between users. Even dating websites and dating applications have become a popular method of meeting people. Use of the Internet to interact with others over social networking platforms has truly created a shift in culture in which online interaction is just as valued, if not preferred, over in-person communication. One of the biggest selling points for many social networking platforms is that users may choose to keep their identities anonymous. Behind the "safety" of their computer screens, many anonymous users reveal much more information about themselves online than they would otherwise share in person. While people's thoughts and behaviors flow freely from their minds to their keyboards, they may be unaware that a large number of social networking companies store copies of their shared information.[41] A comment written out of anger or frustration, or an unflattering or racy picture posted too quickly may be archived to the company's servers for eternity, even if deleted immediately.[42] The more information users willingly share, the more information the companies are able to sort, store, and use at a later date.

Cloud computing has also helped to increase the amount of data stored from online postings. Cloud computing entails "the migration of essential computing and storage facilities from local devices owned by users to distant servers owned by operators."[43] Through web services such as Gmail, Yahoo! Mail, and Hotmail, millions of users and businesses now store many of their emails and messages with third parties rather than downloading each individual message onto their own computer's hard drive or servers.[44] Apple, Amazon, and other

---

[41] *Id.* at 1316.
[42] *Id.*
[43] *Id.* at 1315 (citing Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359, 363 (2010)).
[44] *Id.* (citing Pew Internet & American Life Project, *Use of Cloud Computing Applications and Services* (Sept. 2008), *available at* http://www.pewinternet.org/files/old-

electronic device manufacturers have created cloud systems allowing users to store and share information between multiple devices. For example, the Apple iCloud allows users to save contacts, pictures, messages, and even website bookmarks between the users' laptop, tablet, and smartphone devices.[45] Cloud storage capabilities offer a more convenient storage option for individuals who no longer need to save their information on large, expensive hard drives. As such, users are able to produce more and more data without worrying about where and how to store it, all while the third parties maintain control over the information.

Finally, the development and increased use of smartphones has greatly contributed to the surge in user-generated data.[46] Smartphones satisfy almost all of a person's computing needs on a single device that is always on and always connected to the Internet. Smartphones also allow users to place phone calls, send messages, take pictures, play games, and connect to social media applications. The ease and convenience of smartphones spurred much of the growth in social media and cloud computing services mentioned above. Smartphones contain GPS chips, microphones, and multiple cameras capable of taking still images and moving videos. Never before has it been easier to access and send information than from a device that is almost always with its user. These smartphones "know where you are, who you are with, and what you are doing, saying, and looking at."[47] Smartphones' ease and convenience invite users to communicate through them and share more information than ever before. Meanwhile, these devices are communicating with businesses that continually archive and mine users' data.

As a result of the popularity and wide-spread adoption of cell phones, applications, and the services they provide,, some scholars fear that too much information has been left exposed.[48] It is still unclear how exactly companies use this data today and how they may plan to use the data in the future. Furthermore, the full extent to which the government has been able to access and utilize much of this third party data is yet to be revealed. One thing is for certain: the more

media/Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf (reporting that fifty-six percent of American Internet users "use webmail services such as Hotmail, Gmail, or Yahoo! mail")).

[45] *See iCloud*, APPLE.COM, https://www.apple.com/icloud/ (last visited Nov. 20, 2014).

[46] *See* Ohm, *supra* note 2, at 1314.

[47] *Id.*

[48] *See generally id.* (explaining how the increased amount of user data available to companies and online could, at its extreme, lead to a world without respect for individual privacy).

information we disclose online, the more information that will be available for potential use against us in the future.

b. New Communication Methods Have Left Much of Our Digital Information Exposed

i. To Businesses

Given the novel nature of communication in the digital age, the value and use of what we communicate to each other and to businesses is not entirely known. However, businesses have begun to discover the power of seemingly insignificant bits of information when combined in databases to help form complete pictures of individuals. The development of "big data" is "the use by companies of powerful new data analytics that help companies squeeze more value from their existing data by making inferences."[49] Companies like Google, Apple, and many retailers are able to aggregate data points to learn things about consumer interests and then use that information internally or sell it to advertising firms. In some cases, the companies may be able to learn information that the consumers may not even know about themselves![50]

As this data becomes increasingly valuable, companies make efforts to generate and retain more of it. Google, for example, has now created so many services that consumers can gain all the information they need through interactions with Google alone. They provide email (Gmail), a web browser (Chrome), an Internet search engine (Google), video, music, and voice services (YouTube, Google Play, and Google Voice), maps and GPS services (Google Maps), and their Android smartphone operating system.[51] Through all of these services Google can allegedly track user behavior on 88% of all Internet domains.[52] Google's tremendous market share of user information has made Google very powerful. Each insignificant act, like sending

[49] *See* Ohm, *supra* note 2, at 1316.
[50] VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK AND THINK 58–59 (2013) (telling the story of how a Target sent coupons for baby clothes and cribs to a man's house before his daughter even told him that she was pregnant).
[51] Dewey, *supra* note 2.
[52] *Id.*

an email or searching online, when combined, allows Google to create "something not too far removed from a detailed portrait of your life and interests."[53]

Now that consumers are learning the extent of the data collected and how it can be used, many are concerned that the information could be used inappropriately. While some fear mild breaches, such as invasive marketing techniques,[54] others are worried that their information could potentially leak to those with more severe consequences, such as hackers[55] or the government.

ii. To the Government

Every time technology advances, so must the Fourth Amendment. With the release of every new gadget, the relationship shifts between law enforcement agents and members of the public. Criminals may be able to use the technology to commit crimes, and officers may use the same or additional types of technology to apprehend more criminals. When advances in technology were slower and interacted with traditionally respected realms of privacy, the courts were better able to limit the government's use of sophisticated technology to protect citizens against invasive Fourth Amendment violations.[56] However, now that technology has rapidly

[53] *Id.*

[54] Quain, *supra* note 3 (explaining how many consumers cancelled their subscriptions to OnStar's services after a change in privacy terms allowed for their data to be sold to other companies).

[55] In recent months hackers have been able to penetrate Target and Home Depot's database systems to access customer credit card data and Apple's iCloud remote storage database to access nude photos and other private information. Natasha Bertrand, *Here's What Happened to Your Target Data That Was Hacked*, BUSINESS INSIDER: TECH INSIDER (Oct. 20, 2014, 10:59 AM), http://www.businessinsider.com/heres-what-happened-to-your-target-data-that-was-hacked-2014-10; Dune Lawrence, *Home Depot's Suspected Breach Looks Just Like the Target Hack*, BLOOMBERG (Sept. 2, 2014, 2:58 PM), http://www.bloomberg.com/news/articles/2014-09-02/home-depots-credit-card-breach-looks-just-like-the-target-hack; Timberg, *supra* note 10 ("[Apple's] security took a publicity hit with the leak of intimate photos of celebrities from their Apple accounts in recent weeks.").

[56] *See* Kyllo v. United States, 533 U.S. 27 (2001) (holding that the government's use of a heat-seeking sensor "not in general public use" to determine whether the defendant employed heat lamps in his home to harvest marijuana was a search in violation of the Fourth Amendment).

outpaced the outer limits of previously-existing case law, many, including judges, feel that Fourth Amendment protections have gradually and deliberately been reduced.[57]

The government has prevalently used the Third Party Doctrine to obtain vast amounts of consumer information without violating the Fourth Amendment. The Third Party Doctrine approach was first articulated in *United States v. Miller*.[58] In *Miller*, the court upheld the government's acquisition of financial data from a bank because, "all of the documents obtained, including financial statements and deposit slips, contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[59] Because the financial data had been shared with a third party, the court held that such information could no longer be considered private, and, therefore, the acquisition of this data did not violate a defendant's reasonable expectation of privacy.[60] This approach extended to include phone numbers in *Smith v. Maryland.*[61] In *Smith*, the court affirmed the government's use of a "pen register" to record the numbers dialed on the defendant's phone by reasoning that, "when [petitioner] used his phone, [he] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. . . . The switching equipment that processed those numbers is merely the modern [equivalent of an operator]."[62] By using such language, the court articulated a clear, categorical rule: "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[63] From these cases and their progenies, it is clear that consumers assume the risk that any information used in third party transactions can be disclosed to law enforcement. This is

[57] *Pineda-Moreno*, 617 F.3d at 1126–27 (Reinhardt, J. dissenting) ("I regret that over [the three decades] the courts have gradually but deliberately reduced the protections of the Fourth Amendment to the point at which it scarcely resembles the robust guarantor of our constitutional rights we knew when I joined the bench. . . . These decisions have curtailed the 'right of the people to be secure . . . against unreasonable searches and seizures' not only in our homes and surrounding curtilage but also in our vehicles, computers, telephones, and bodies—all the way down to our bodily fluids and DNA.").
[58] 425 U.S. 435 (1976).
[59] *Id.* at 442.
[60] *Id.* at 443.
[61] Smith v. Maryland, 442 U.S. 735 (1979).
[62] *Id.* at 744.
[63] *Id.* at 743–44.

true even when exposing information to friends and family members with the belief "that it will be used only for a limited purpose and [that the declarant's] confidence placed in the third party [would] not be betrayed."[64]

In the traditional cases that involved government informants or access to one particular type of information, such as bank records, the Third Party Doctrine appears palatable. However, with the development of technology and the increase in the type and quantity of information disclosed to third parties, the Third Party Doctrine has provided a windfall of information to the authorities. In response to the recent availability of previously inconceivable amounts of information, some judges, including Supreme Court Justice Sotomayor, have suggested reconsidering the Third Party Doctrine's mantra that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.[65] Many individuals, scholars, judges, and lawmakers fear that the government's unbridled access to these vast quantities of data, if unchecked, could lead to abuses of power and the rise of a "surveillance society."[66]

Edward Snowden's disclosures of the National Security Agency's ("NSA") activities prompted the most recent and prevalent concerns regarding governmental power abuses in obtaining information. Beginning in 2002, President George W. Bush secretly authorized the

---

[64] *Miller*, 425 U.S. at 443; *See also* United States v. Jacobsen, 466 U.S. 109, 117 (1984) ("It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities."). For a list of the many situations in which an individual has no constitutionally protected expectation of privacy under the Third Party Doctrine, *see* ACLU v. Clapper, 959 F. Supp. 2d. 724, 749–51, n.16 (S.D.N.Y. 2013) *aff'd in part, vacated in part, remanded*, 785 F.3d 787 (2d Cir. 2015).

[65] United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("[The Third Party Doctrine] 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. 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. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they have visited in the last week, or month, or year.").

[66] *See generally* Ohm, *supra* note 2, at 1310-20; *see also* Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 127 (2008) ("Freedom requires that people be able to live their personal lives without a pervasive, cringing fear of the state. A fear produced by the justified apprehension that their personal lives are subject at any moment to be violated and indeed taken from them if they become suspicious in the eyes of governmental authorities.").

NSA, in certain circumstances, to intercept Americans' telephone calls and e-mail messages without probable cause or a court order.[67] As a result, the NSA began to access communications data from "tens of millions" of presumably innocent people.[68] In 2013, Edward Snowden revealed that the government had not only been collecting the data of "tens of millions" of people, but telephone metadata from *everyone* through its bulk telephony metadata collection program.[69] Such telephony metadata includes "the telephone numbers that placed and received the call, the date, time, and duration of the call, other session-identifying information . . . trunk identifier, and any telephone calling card number."[70] When combined, all of this metadata allows the government to uncover a "rich profile of every individual as well as a comprehensive record of people's associations with one another."[71] The use of this data-surveillance program by the NSA, deemed lawful by analogy to the Third Party Doctrine,[72] has incited fears that government oversight has grown too invasive.[73] However, telephony metadata is not the only thing that the government is able to collect.

Through deployment of the Third Party Doctrine, the government has access to almost all of the information revealed to each of the businesses mentioned in the sections above. In

---

[67] Rubenfeld, *supra* note 66, at 102-03.
[68] *Id.*
[69] *ACLU*, 959 F. Supp. 2d at 730 ("[The bulk telephony metadata collection program] only works because it collects everything. . . . Each time someone in the United States makes or receives a telephone call, the telecommunications provider makes a record of when, and to what telephone number the call was placed, and how long it lasted. The NSA collects that telephony metadata.").
[70] *Id.* at 734 (citation omitted).
[71] *Id.* at 730.
[72] *Id.*; *but see* Klayman v. Obama 957 F. Supp. 2d 1, 32 (D.D.C. 2013) (holding that the Third Party Doctrine is not applicable to mass surveillance the scale of the NSA bulk telephony metadata collection program and as a result violates an individual's reasonable expectation of privacy.).
[73] *See* Jamie Rigg, *Blackphone Review: Putting a Price on Privacy*, ENGADGET.COM (Oct. 3, 2014, 3:00 PM), http://www.engadget.com/2014/10/03/blackphone-review/ ("As Edward Snowden continues to leak information about how the NSA and other national government agencies were/are hoovering up every bit of personal data available to them, digital privacy has never been a hotter topic."); Michael Isikoff, *FBI Tracks Suspects' Cell Phones Without a Warrant*, NEWSWEEK (Feb. 8, 2010, 7:00 PM), http://www.newsweek.com/fbi-tracks-suspects-cell-phones-without-warrant-75099 ("[C]ell-phone tracking is among the more unsettling forms of government surveillance, conjuring up Orwellian images of Big Brother secretly following your movements through the small device in your pocket.").

addition to bank records and telephony metadata, the government can collect a person's social media posts, pictures, email metadata, and even their locational information.[74] Not only does the government have access, but they frequently take advantage of that information and have "exponentially" increased requests for more.[75] No longer does the government need to follow a suspect and record the data points themselves. Instead, the government is able to save resources by taking a backseat to the telecommunications companies and allowing the private sector to turn over everything the government needs.[76] Because of the government's relatively unhindered access to vast amounts of information, many fear abuse.[77]

This vast and seemingly limitless government power to collect "private" user information has instigated some pushback from the judiciary, as many judges have begun to question the proper extension of the Fourth Amendment and the Third Party Doctrine in a continually changing technological landscape.[78] It has long been accepted that an officer may follow

---

[74] *See Privacy Policy* [hereinafter *Apple Privacy Policy*], APPLE, https://www.apple.com/legal/privacy/en-ww/ (last accessed Nov. 5, 2014) ("It may be necessary—by law, legal process, litigation, and/or requests from public and governmental authorities within or outside of your country of residence—for Apple to disclose your personal information. . . . Apple and our partners and licensees may collect, use, and share precise locational data, including real-time geographic location of your Apple computer or device.").

[75] *See* Isikoff, *supra* note 73 (explaining that wireless providers are now receiving "thousands" of information requests per month and that the amount has grown "exponentially" over the past few years).

[76] *See* Ohm, *supra* note 2, at 1322 ("It is as if today's FBI has developed a sophisticated research-and-development arm with field offices named Apple, Google, Facebook, Comcast, and AT&T. On the surface, these private labs seem similar to FBI labs with big buildings and smart engineers. But peel back a layer and it is obvious that these abs can do something important that no FBI lab could ever hope to do—convince the surveillance targets of the world to consensually adopt their surveillance technologies, acting as a neat end-around circumventing the Fourth Amendment.").

[77] *See* Isikoff *supra* note 73 (detailing one incident of abuse in which a local Alabama sheriff called a telecommunications company to demand they ping his daughter's cell phone every few minutes in order to identify her location and another where Michigan police demanded telecommunications information from all cell phones congregating in the area of an expected labor-union protest due to fear of a "riot").

[78] *See e.g.*, United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring); *Id.* at 962 (Alito, J., concurring) ("Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. 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

someone on the street or that an undercover agent or informant may coax out "private" information, but it is entirely different for citizens to feel as though they're operating under Big Brother's all-seeing, never sleeping gaze.[79] Unfortunately, the Supreme Court has not limited the Third Party Doctrine's application to digital information exposed to a telecommunications company. As a result, the public has acted in accordance with Judge Clement of the Fifth Circuit's advice by turning to the private sector to quiet their fears.[80]

c. In Response to this Exposure, A Market for Privacy-Protecting Goods and Services Has Emerged

i. Privacy as a Commodity

The term commodity refers to goods and services that are "distributed through the bargaining mechanisms of a marketplace where those goods and services are sold."[81] Once in the marketplace, the commodity will be distributed according to financial means: those willing and able to pay the most will be the ones who receive it.[82] As mentioned in Part I, historically, privacy can be bought through physical goods and services. A person able to purchase a large stand-alone house on a large lot, to build a fence around their backyard, or to hire security guards

---

welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.");

[79] United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, J., dissenting) ("You can preserve your anonymity from prying eyes, even in public, by traveling at night, through heavy traffic, in crowds, by using a circuitous route, disguising your appearance, passing in and out of buildings and being careful not to be followed. But there's no hiding from the all-seeing network of GPS satellites that hover overhead, which never sleep, never blink, never lose attention. Nor is there respite from the dense network of cell towers that honeycomb the inhabited Unites States.").

[80] In re U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) ("We understand that cell phone users may reasonably want their location information to remain private, just as they may want their trash, placed curbside in opaque bags, or the view of their property from 400 feet above the ground, to remain so. But the recourse for these desires is in the market or the political process: in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections.").

[81] Robin M. Collin & Robert W. Collin, *Are the Poor Entitled to Privacy?*, 8 HARV. BLACKLETTER J. 181, 202 (1991).

[82] *Id.*

can be secluded and maintain a private and intimate space. Therefore, privacy is a commodity that can be sold to the highest bidder.[83]

Just as a person could historically purchase privacy in their physical space, a market is now developing for the purchase of digital privacy. Many companies are realizing that they must compete for consumers by creating a reputation that their products and services will protect users from unbridled government data collection.[84] Snowden's NSA disclosures revealing the quantity of information collected and stored by the government has intensified public concern and anxiety regarding government oversight, especially given the number of people that were being watched without cause. As a result, companies have grown increasingly determined to show that they prize their relationships with their customers over their relationships with the government.[85]

[83] *See* ANITA ALLEN, UNEASY ACCESS 61 (1988) ("It is plain that in the United States domestic privacy is a virtual commodity purchased by the middle class and the well-to-do. Privacy is bought and sold in the form of single-family houses on privately-owned land, townhouses, apartments, and recreational second-homes in remote locations. . . . Economic status can also affect enforceability of privacy-related rights against trespass and to seclusion at home.").

[84] Craig Timberg, *Apple, Facebook, Others Defy Authorities, Increasingly Notify Users of Secret Data Demands After Snowden Revelations*, WASH. POST (May 1, 2014), http://www.washingtonpost.com/business/technology/apple-facebook-others-defy-authorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html ("Fueling this shift [in a defiant industry stand against the government] is the industry's eagerness to distance itself from the government after last year's disclosures about the [NSA] surveillance of online services. Apple, Microsoft, Facebook and Google are all updating their policies to expand routine notification of users about government data seizures, unless specifically gagged by a judge or other legal authority.").

[85] *Id.*; *See also* Timberg, *supra* note 10 ("Particularly after the Snowden disclosures, Apple seems to understand that consumers want companies to put their privacy first.").

Companies have updated their privacy policies,[86] offered new products and services,[87] and in some cases even publicly sued the government.[88]

ii. Examples of New Products and Services in the Market

Many companies have recognized a shift in consumer preference for certain qualities and services. In order for companies to compete and maintain their customer base during the release of new and improved technologies, they now must acknowledge that consumers are looking for improved privacy protection in addition to improved hardware and software. Apple and Google, two of the largest and most influential technology companies, have recently released new versions of their smartphones with operating systems that immediately begin encrypting the cell phone's sensitive data – such as mail, text messages, photos, and call records – as soon as the user creates a lock passcode.[89] Further, Apple has refused to create a "back door" passcode to this encryption, which would allow them to hack into phones from their servers. By so doing,

[86] *See Apple Privacy Policy*, *supra* note 74 ("Apple has never worked with any government agency from any country to create a 'back door' in any of our products or services. We have also never allowed any government access to our servers. And we never will."); Timberg, *supra* note 10 ("Tech companies [are attempting] to blunt allegations that they have too readily participated in government efforts to collect user information.")

[87] *See* Juliam Hattem, *FBI 'Very Concerned' About iPhone Lock*, THEHILL.COM (Sept. 25, 2014, 3:25 PM), http://thehill.com/policy/technology/218931-fbi-very-concerned-about-iphone-lock ("Last week, both Apple and Google announced that the new iPhones and Android devices would automatically come loaded with encryption technology automatically preventing anyone without a passcode – even police holding a warrant – from accessing pictures, notes, and other messages on the phone. . . . This move is part [of] an increasing trend . . . for companies to compete with one another to boost privacy, and was greeted enthusiastically by civil liberties advocates.").

[88] *See* Ellen Nakashima, *Twitter Sues U.S. Government Over Limits on Ability to Disclose Surveillance Orders*, WASH. POST (Oct. 7, 2014), http://www.washingtonpost.com/world/national-security/twitter-sues-us-government-over-limits-on-ability-to-disclose-surveillance-orders/2014/10/07/5cc39ba0-4dd4-11e4-babe-e91da079cb8a_story.html.

[89] Matthew Green, *Is Apple Picking a Fight With the U.S. Government?*, SLATE.COM (Sept. 23, 2014, 10:51 AM), http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html.

the company has made it impossible for the government, with or without a warrant, to compel the company to turn over encrypted data.[90]

Existing companies are not the only ones who have begun to introduce improved privacy-protecting technologies. New companies are taking advantage of this opportunity and have begun to form a new privacy-protection industry.[91] One of the most popular new products has been the Blackphone, which claims to be an "unparalleled [smartphone] where data protection is concerned."[92] The phone runs on a specially made Android operating system that prevents all Google integration; there is no connectivity to the "app store," maps, or anything else outside basic smartphone functions.[93] This bare-bones device and operating system is then paired with "leading applications optimized for security."[94] Some applications included with Blackphone (also available separately) are Silent Circle (a bundle of secure communications applications), Disconnect Secure Wireless (an application that routes any internet traffic through a VPN if it detects an unsecured network), and SpiderOak (a secure cloud-storage service).[95] Though Blackphone has only been in the market since June 2014, sales of the device have been surprisingly strong.[96] Another product, Integricell, which allegedly warns users when police and intelligence agencies are utilizing mobile surveillance equipment to track their movements and monitor their calls, has also proven to be a popular item.[97] Finally, a person concerned with

---

[90] *See Apple Privacy Policy*, *supra* note 74; Hattem, *supra* note 86. It is important to note that this new technology is not designed specifically for the purpose of keeping out the government, as encryption protects against other forms of data hacking as well. *See* Timberg, *supra* note 10 (explaining how Apple wishes to redeem itself as a company that protects customer privacy after intimate celebrity photos were hacked from their Apple accounts earlier this year).

[91] Rigg, *supra* note 73 (reviewing the myriad new goods and services available for customers who "want to stay off the grid without going offline"); *see* Reilly, *supra* note 6 (highlighting the remarkable convergence of market opportunity with the release of new ultra-secure products and services).

[92] Rigg, *supra* note 73.

[93] *Id.*

[94] Reilly, *supra* note 6.

[95] *See* Rigg, *supra* note 73.

[96] Reilly, *supra* note 6 ("Sales of [the] new ultra-encrypted smartphone, Blackphone, are flying off the shelves since it began officially shipping in June."); Angwin, *supra* note 1 ("Blackphone . . . is being pre-ordered by the thousands.").

[97] Ashkan Soltani & Craig Timberg, *Tech Firm Tries to Pull Back Curtain on Surveillance Efforts in Washington*, WASH. POST (Sept. 17, 2014),

protecting their voice calls could be interested in JackPair, which attaches to a user's headphone jack to encrypt the contents of their voice call.[98]

d. This Market for Privacy-Protecting Goods and Services Creates a Discrepancy in Protections Across Class Lines

Like the fences, large houses, and security guards that protect physical privacy, many of the new digital privacy products and services cost money. For example, the most basic version of Apple's iPhone 6 with encryption capabilities costs $199 with a two-year service contract and $649 without a contract.[99] The cost of Blackphone, which doesn't have an option to purchase under service contract, costs $629.[100] The secure applications preloaded on the Blackphone can only be used for one year, and additional downloadable applications must be ordered by subscription ranging from $3 to $40 or more per month.[101] Integricell, which arguably provides the most security against government intrusion, sells at $3,500 per unit.[102] Finally, even the "cheaper" of the devices at $89 per set, JackPair, must be owned by the users of both phones in order for the voice call encryption to be effective.[103] As a result, many consumers, even those concerned about protecting their privacy and preventing unreasonable government searches, will be barred from protecting their information in the same way as those who *can* afford these products and services.[104]

Though some products and services in the marketplace do not cost money, many individuals still suffer disparate privacy protections from a lack of knowledge about available

---

http://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html (explaining the features of Integricell and noting that the new company has already sold 30,000 units in the United States and 300,000 units globally).

98 Natasha Lomas, *JackPair Lets You Encrypt Voice Calls Whatever Phone You're Using*, TECHCRUNCH.COM (July 31, 2014), http://techcrunch.com/2014/07/31/jackpair/.

99 Apple Store, APPLE.COM, http://store.apple.com/us/buy-iphone/iphone6 (last accessed Nov. 15, 2014).

100 Rigg, *supra* note 73.

101 *Id.*

102 Soltani & Timberg, *supra* note 97.

103 Lomas, *supra* note 98.

104 Angwin, *supra* note 1 (detailing the account of one individual who spent countless hours and over $2,200 in one year to purchase products that would protect her private, digital information).

technologies and how to use them. First, people must know that the government is able to access their digital information. According to some privacy advocates, most of the nation's 277 million cell phone owners do not know that their telecommunications companies can track the location of their devices in real time.[105] Further, even fewer understand the extent of the government's capabilities to obtain this information under the Third Party Doctrine.[106] Even if members of the public do understand the extent to which their information may be compromised, they must then understand how to download and utilize the various encryption and data-protecting services available to them. Thus, regardless of their ability to pay, those that lack knowledge of their data's availability to the government or the privacy-protecting technology available will be unprotected.

The current Fourth Amendment doctrine, as applied to one's interest in their digital information under the Third Party Doctrine, has allowed the government to gain access to substantial amounts of data. This seemingly unrestricted access had made many individuals feel very uncomfortable – so uncomfortable, in fact, that a market for privacy-protecting goods and services has emerged where the judiciary has failed to limit application of the doctrine. Often times these products are new, cutting-edge, and extremely expensive. Even if they are not expensive, a person must have knowledge of their existence and be able to effectively utilize the hardware or software. As a result, only those able to afford these services or who know how to employ them are afforded the proper privacy protections. Therefore, under the current law, those with less knowledge about these products and less disposable income are afforded fewer privacy protections over their digital information than those with greater knowledge and means.

III. The Protection of Digital Privacy Across Class Lines is Problematic

The disparity in Fourth Amendment privacy protections across class lines is troublesome. First, the idea that constitutional protections can vary depending on the individual is worrying because it violates the concept of a constitutional guarantee. The courts' decisions have granted unprecedented levels of access to large quantities of digital information, limiting the Fourth

---

[105] Isikoff, *supra* note 72.

[106] United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, J., dissenting) ("Most targets won't know they need to disguise their movements or turn off their cell phones because they'll likely have no reason to suspect that Big Brother is watching them.").

Amendment's protections over such information and creating a private sector market for goods to protect privacy where the Constitution has failed to do so. These decisions have turned the constitutional right to privacy into a commodity. A constitutional guarantee assures that a particular right or interest will be protected from all intrusions, including those by the government.[107] It is the government's duty to ensure, as far as its own conduct is concerned, that "these guarantees are shared by all Americans regardless of profit or money."[108] Consequently, the courts have allowed market forces to distribute this constitutional right rather than ensuring the right across all economic classes. Since poor people do not have the same access to the private market for goods and services as wealthier members of society, the analysis adopted by the courts has unevenly distributed privacy protections across class lines. This is problematic because "a constitutional guarantee is a statement that a certain right or interest is too important to be distributed according to profit, and the costs of equitable redistribution of such a right or interest throughout society must be borne [by all]."[109] In allowing this right to be distributed according to profit rather than equally throughout society, the analysis adopted by the courts has violated the purpose and concept of a constitutional guarantee.[110]

Second, the disparate coverage of constitutional protections across class lines offends American morals and virtues. Through the Constitution and the Bill of Rights, Americans have "a common denominator of certain fundamental rights which characterizes American virtues."[111]

---

[107] Collin & Collin, *supra* note 81, at 189.
[108] *Id.*
[109] *Id.*
[110] It may also be argued that beyond violating the initial purpose and concept of a constitutional guarantee, the distribution of a right according to profit violates the Equal Protection Clause of the Fourteenth Amendment. The Fourteenth Amendment is usually cited as guidance for the legislature that some model of equality and equal treatment be met in order for legislation to be valid. Collin & Collin, *supra* note 81, at 183-84 n.13. Violations of the Equal Protection Clause are typically evaluated based on the group of people being discriminated against. At a minimum, equal protection demands a rational basis between legislative purpose and the difference in treatment between the various groups. However, certain classifications and differences in treatment require strict scrutiny and are deemed presumptively improper when they are derived from prejudice against discreet and insular minorities. United States v. Carolene Products Co., 304 U.S. 144, 153, n.4 (1938). Though race and some other classifications have received strict scrutiny analysis, poverty has never been recognized as such a group. Collin & Collin, *supra* note 80, at 183-84 n.13.
[111] *Id.* at 189.

Since this country consistently stands for the proposition that certain rights are essential to those living in a free and decent society, the protection of these fundamental rights – through the guarantee that they are enjoyed by all, regardless of means – is as much a social need for the integrity of our society as it is a personal need for the individual. Once the availability of a constitutional right depends upon economic means, these fundamental rights no longer represent American values, but instead, merely represent the sum of the nation's possessions.

Third, the unequal distribution of privacy protections violates the original purpose of the Fourth Amendment. Some judges and scholars believe that the Fourth Amendment was developed to protect against "general warrants," which allowed British troops to search people and homes indiscriminately and without suspicion.[112] However, while on the surface these indignities appear to reflect privacy concerns, the drafters were arguably more concerned with redefining their relationship of insecurity with the state and correcting an imbalance of power.[113] The founders were worried about tyranny and the centralization of government power; they believed that the citizenry should be skeptical of government power because people in power cannot always be trusted.[114] Echoing the founder's fears, Edward Snowden's NSA disclosures have caused many American citizens to start fearing excessive government oversight. Many new products and services to protect against government intrusion were created and introduced into the marketplace as a result of this emerging sense of fear and mistrust of government's power[115]—a fear that that the public's personal lives will be "subject at any moment to be violated and indeed taken from them if they become suspicious in the eyes of governmental authorities."[116] This apprehension of government power, which has the potential to chill activity and create insecurity among the people, is exactly what the founders sought to avoid. By allowing the market—rather than the Fourth Amendment—to dictate which individuals may avoid fear of excessive government oversight, the original purpose of the Fourth Amendment is frustrated.

---

[112] Ohm, *supra* note 2, at 1334.
[113] *Id.*
[114] Comey, *supra* note 5.
[115] Rigg, *supra* note 73 (explaining how many of these companies selling privacy products are actually selling "peace of mind" against improper government oversight).
[116] Rubenfeld, *supra* note 66, at 127.

Fourth, the division of privacy protections across class lines disturbs the overall workability and application of the "reasonable expectation of privacy" doctrinal analysis. Determination of one's reasonable expectation of privacy should not hinge on what types of protections a person is able to afford. In order to allow government access to digital information, the courts have applied the outdated logic that once this information is voluntarily conveyed to service providers, a person no longer has a reasonable expectation of privacy in such data.[117] However, there exists the possibility that, over time, many more people will begin to purchase the Blackphone or own smartphones that automatically encrypt data, like in the iPhone 6. Consumer reclamation of their privacy interests in their digital information through purchases of privacy-protecting devices directly contradicts the notion articulated by the courts. At what point do consumers as a whole reclaim their "reasonable expectation of privacy" so as to eliminate feasible application of the Third Party Doctrine? Over time, it will become increasingly difficult to draw the line between when a person's expectation of privacy in their digital information is reasonable and when it is not. Until the prices of these products have decreased or until enough people adopt these services so as to force the courts to rethink their doctrinal analysis, those unable to afford these services will remain at a disadvantage.

Finally, the discrepancy of protection across class lines will impact the economics of policing crime such that searches of poorer individuals will disproportionately rise compared to searches of their wealthier counterparts. In a society with limited law enforcement resources, the police must necessarily pick and choose which offenses to investigate. Anything that makes one set of crimes more expensive to investigate serves to make other sets of crimes comparatively cheaper.[118] By turning people to the market for protection, rather than distributing privacy protections equally across society, the courts have created a landscape in which it will now be more expensive for police to investigate certain individuals over others. For example, it would take upwards of five years to guess a 6-digit password on Apple's new encryption software.[119] As a result, where the police must choose between searching a person with a brand new iPhone 6 or a person with an older or less-secure smartphone or computer, the police will likely select the

---

[117] *See supra* Part II.b.ii (explaining the third party doctrine and its application to digital information).
[118] Stuntz, *supra* note 16, at 1274.
[119] Green, *supra* note 89.

cheaper search. As more and more people begin to adopt and purchase these privacy-protecting devices and services, law enforcement will increasingly turn towards investigating only those unable to afford these expensive products. Therefore, because the current Fourth Amendment doctrine protects the wealthy so well, these class-tilted protections may ultimately cause poorer individuals to be subjected to searches far more than their wealthier counterparts.[120]

IV. Solutions

There are a few possible solutions for mitigating the problems created by unequal access to digital privacy protections. The first is to acknowledge that since many people are turning to the market for privacy protections, the solution may be the market itself. If a lack of awareness about the type, quantity, and frequency of information disclosed to companies and to the government is a problem, companies should be more candid in their privacy policies regarding that disclosed information. Such openness could allow consumers the ability to make the conscious choice of not disclosing their private information to companies in the first place. However, this notion may not be feasible. First, companies may not be able to be forthcoming regarding what types of information and how much of it is being disclosed to the government because they themselves may not know until presented with an information request.[121] Also, companies may not want to be forthcoming regarding information disclosures because a liberal privacy policy may hurt their reputation in the marketplace.[122] Second, even if this information was provided more clearly and openly to consumers, there is no guarantee that consumers will be able to use it to make wise decisions about what information to "reveal." People rely on the Internet and other technological innovations as a source of information, commerce, and communication, so people may not be able to alter their behavior to avoid privacy vulnerabilities. For example, without access to phones or the internet, people have to communicate in person. The feasibility of driving or flying to someone else's home in order to communicate in person is especially burdensome for those who would need to make these efforts in the first place—i.e.,

---

[120] *See* Stuntz, *supra* note 16, at 1287.
[121] *See* James B. Comey, Dir., Fed. Bureau of Investigation, The FBI and the Private Sector: Closing the Gap in Cyber Security, Speech Before the RSA Cyber Security Conference (Feb. 26, 2014), http://www.fbi.gov/news/speeches/the-fbi-and-the-private-sector-closing-the-gap-in-cyber-security.
[122] *See id.*; Quain, *supra* note 3.

those who cannot afford the privacy goods and services in the marketplace. As a result, increasing awareness regarding information disclosures is unlikely to provide relief.

Another suggestion in the marketplace could be to make these products available to everyone, or at the very least to make them more affordable. If everyone owned a JackPair voice-encryption device then no one would be afforded greater protection over anyone else. However, this too will likely be infeasible. Many of these products and services require the employment of cutting edge technology in a rapidly evolving and innovative market. As a result, the costs of research, development, and maintenance of up to date and effective encryption and decryption software are very expensive. Encryption technology is a lucrative field that requires highly specialized knowledge, and it is therefore unlikely that these companies can or will provide these products and services for free or at reduced costs to the public. However, even free or "more affordable" products would still run into the problem of public awareness about these products' existence and how to use them. Additionally, if everyone adopted more advanced privacy technologies, law enforcement's ability to quickly and effectively fight crime could be undermined. More sophisticated privacy technology would allow criminals to become more sophisticated in their communications between one another and that much more difficult to intercept. Law enforcement must be able to keep up with and detect these criminals, sometimes before a crime occurs, in order to effectively keep the public safe. Arguably, if everyone owned an iPhone 6 that required five years or more to decrypt, the effectiveness of law enforcement in fighting crime could be frustrated.[123]

If no feasible solutions appear from the market, a reevaluation of Fourth Amendment doctrinal analysis may be more appropriate. One possibility may be to reconsider the way in which the courts have traditionally defined "privacy." Some scholars argue that by giving privacy a positive definition, such that the privacy protection citizens have with the police is tied to the kind of privacy citizens have between one another, the doctrine will tend to favor certain types of people over others.[124] However, perhaps the definition of privacy should be more

---

[123] *See* Comey, *supra* note 5 (detailing the difficulties balancing an individual's interest in their digital information and the public's perception of government surveillance against the government's need for that information to effectively fight sophisticated criminals).
[124] Stuntz, *supra* note 16, at 1267.

normative: instead of examining what privacy we *actually* have between one another, we should ask what privacy we *ought* to have with the police.[125] That way, the law will be able to provide the same levels of privacy protections against police to everyone, equally.

Another solution is to reevaluate the applicability of the Third Party Doctrine to a person's interests in their digital information.[126] One argument against applying the Third Party Doctrine is that the courts simply lack the institutional competence to appreciate, in times of technological flux, whether the government has violated a subjective expectation of privacy that society has deemed reasonable.[127] They lack the information needed to understand how new technologies work, how consumers interact with these new technologies, and how the technologies fit into a greater technological landscape.[128] As a result, the courts cannot and should not apply the Fourth Amendment to changing technologies until the technology "stabilizes."[129]

Beyond limitation of the overall use of the Third Party Doctrine, courts should specifically reduce its applicability to digital information by distinguishing the information "voluntarily disclosed" in 2014 from the type and amount of information disclosed in the past.[130] The leading cases for the creation of the Third Party Doctrine, *Smith* and *Miller*, both occurred over thirty years ago. *Smith* involved the use of a "pen register" to record the numbers dialed on a phone, and *Miller* involved access to an individual's bank information. Each case involved only one type of information, in a certain, limited quantity that was voluntarily disclosed to the third party. However, the Supreme Court in both of those cases could not have imagined the widespread use

---

[125] *Id.* at 1272.
[126] Ohm, *supra* note 2, at 1331.
[127] *See* Orin Kerr, *The Fourth Amendment and New Technologies*, 102 MICH. L. REV. 801, 807 (2004) ("Judicial decisions tend to incorporate outdated assumptions of technological practice, leading to rules that make little sense in the present or future. Courts also lack the information needed to understand how the specific technologies in cases before them fit into the broader spectrum of changing technologies, and cannot update rules quickly as technology shifts.").
[128] *Id.*
[129] *Id.* at 805.
[130] One of the most recent cases attempting to limit the applicability of the Third Party Doctrine by distinguishing current facts from those in the 1970s is *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated*, 800 F.3d 559 (D.C. Cir. 2015), *remanded to* 142 F. Supp. 3d 172 (D.D.C. 2015) (holding that the NSA's bulk telephony metadata collection program does not fall under the rationale of the Third Party Doctrine and as a result constitutes an unreasonable search under the Fourth Amendment).

of the Internet, or the availability of smartphones and how consumers would interact with their phones, in the current digital age. The pen register in *Smith* recorded data on one person for a few days, but current day companies (and the government by extension) are able to record much more information, on many more people, for a seemingly unlimited duration of time.[131] Additionally, the relationship between the government and the telecommunications company in *Smith* is different from the way the government interacts with information services companies today. In *Smith*, the government asked for the phone company's permission to install the pen register in order to record the numbers the defendant dialed from his home.[132] In contrast, today's government is sometimes supplied large quantities of information in what could be perceived as a "joint intelligence-gathering operation."[133] The government no longer needs to investigate crimes by installing pen registers itself. Rather, it can simply let the Third Party Doctrine do all the work of collecting information and simply sit back and look at all the data sent to it by private companies.[134] This change in the information technology landscape, and shift in power between individuals, information services companies, and the government, were likely unforeseen by the Court when deciding the original Third Party Doctrine cases of *Miller* and *Smith.* As such, those cases should be distinguished from current-day surveillance techniques under the Third Party Doctrine whenever possible. Such an analysis would limit the amount of information the government can access and thereby limit the extent to which consumers will turn to the market to protect their privacy interests.

Conclusion

The more technology increases a user's quality of life, the more it will be adopted, utilized, and relied upon by members of society. As can already be seen, technological advancements of the past few years have transformed a person's cell phone or social network profile into a reflection of their personality. The more that technology is used, the more information people reveal to the companies behind those services. Through the courts' continual expansion of the

---

[131] *See id.* at 33.
[132] Smith v. Maryland, 442 U.S. 735, 737 (1979).
[133] *Klayman*, 957 F. Supp. 2d at 33.
[134] *See generally* Ohm, *supra* note 2 (explaining how the Third Party Doctrine has allowed the government to simply subpoena private companies for information that it previously needed to collect itself).

Third Party Doctrine, the government has been able to access much of this "revealed" information. In response to fears of unbridled government oversight, a market for privacy-protecting goods and services has developed for purchase of products that encrypt and protect personal data. Unfortunately, since constitutionally protected privacy is limited to that which individuals can protect behind effective barriers to intrusion, those with lesser means are able to erect fewer "barriers to intrusion" against the government than their wealthier counterparts. As a result, some members of society are disparately afforded fewer constitutional protections than others. This disparity is problematic for a number of reasons, one of which is that it may cause cost-conscious law enforcement agents to search the digital information of poorer individuals more frequently than that of the wealthy, who can protect themselves with greater and costlier to penetrate privacy protections. Fortunately, fears of a surveillance society can still be allayed while simultaneously providing equal Fourth Amendment protections to all by limiting the government's access to data under current doctrine. So long as the court begins to consider the greater implications of their decisions on the market and how various members of society may be impacted, any disparity in protections across class lines will hopefully be mitigated or eliminated altogether.