THE FOURTH AMENDMENT IN A WORLD WITHOUT PRIVACY

*Paul Ohm**

* Associate Professor, University of Colorado Law School. I thank the National Judicial Center and the *Mississippi Law Journal* for the invitation to participate. I specifically thank Tom Clancy for being the driving force behind this symposium, the essential annual forum for scholarly debate about the Fourth Amendment, one that deserves to continue for many years. Thanks also to Nicole Friess for research assistance.

INTRODUCTION

If we woke up tomorrow in a nation without privacy, one in which powerful companies watched the moves of every citizen, with the full awareness and consent of the watched, would the Fourth Amendment still apply? Does that amendment's "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"[1] survive once the police can request from the private sector the fruits of comprehensive, consensual private surveillance? Were we unthinkingly to extend current Fourth Amendment doctrine, the answer to these questions might be no. If we woke up tomorrow in a world without privacy, we might also find ourselves in a world without constitutional protection from new, invasive police powers. This bleak scenario is not science fiction, for tomorrow we will likely wake up in that world.

Every year, companies, especially those that deliver services online, spend millions of dollars developing new services that track, store, and share the words, movements, and even the thoughts of their customers.[2] These invasive services have proved to be irresistible to consumers, who have voluntarily embraced them in droves launching a social age of self-revelation. Millions now own sophisticated tracking devices (smartphones) studded with sensors and always connected to the Internet. They have been coaxed to use these devices to access fun and valuable services to share more information, more of the time. Our country is rapidly becoming a surveillance society.

---

[1] U.S. CONST. amend. IV.

[2] *See* discussion *infra* Part I.

Meanwhile, the police can access the records that the surveillance society produces and stores with few impediments. Current Fourth Amendment doctrine—premised on the reasonable expectation of privacy test and elaborated through principles such as assumption of risk, knowing exposure, and general public use—places far fewer hurdles in front of the police when they use the fruits of somebody else's surveillance than when they do the surveillance themselves. As the surveillance society expands, the police will learn to rely more on the products of private surveillance, and will shift their time, energy, and money away from traditional self-help policing, becoming passive consumers rather than active producers of surveillance. Private industry is destined to become the unwitting research and development arm of the FBI. If we continue to interpret the Fourth Amendment as we always have, we will find ourselves not only in a surveillance society, but also in a surveillance state.

This Article explores the relationship between private and public surveillance. In one sense, this is well-trodden ground, as many Criminal Procedure scholars have written about this relationship, especially in debates over the Fourth Amendment's third-party doctrine.[3] But few of these scholars have followed the creeping trend lines of technological evolution all the way to where they seem to be headed. Systems of private surveillance are not simply becoming more powerful and widespread, but they are becoming all-knowing and ubiquitous. What might have seemed like a slow and partial degradation of the Fourth Amendment appears instead to be a full evisceration.

But if we believe that the Fourth Amendment can and should survive the coming reach of private surveillance, it is not enough to prescribe mild tweaks to the third-party doctrine. A more thorough reinvention of the Fourth Amendment is in order. We should rebuild the Fourth Amendment atop a foundation of something other than privacy, and this Article extends the work of others who have searched for alternative theoretical underpinnings for the amendment. These scholars have convincingly suggested that

---

[3] Professor Orin Kerr quipped that "[a] list of every article or book that has criticized the [third-party] doctrine would make . . . the world's longest law review footnote." Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 n.5 (2009) (listing representative examples).

the Fourth Amendment was originally intended and is better interpreted to ensure not privacy but liberty from undue government power. For more than two hundred years, privacy has served as a pretty good proxy for this value, but the 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.

The good news is that the work of these scholars will soon take center stage, because judges are not likely to lash the Fourth Amendment to the sinking ship of privacy. The bad news is that these scholars have not yet done enough to turn their principles into concrete rules, and most importantly, they have failed to offer a workable new test to replace the venerable reasonable expectation of privacy test. Any judges convinced to shift the Fourth Amendment from privacy to liberty and power will find little in legal scholarship to help them turn their conviction into a rule.

Orin Kerr has recently offered a promising theory to fill this void. He calls it "equilibrium adjustment," the idea that Fourth Amendment rules are tailored to preserve a level playing field between the police and criminals facing technological change.[4] I embrace this theory as not only a convincing description of what courts have done but also a normatively desirable theory of what courts should do.

But I improve on Kerr's version of the equilibrium-adjustment theory, which does a good job explaining the Fourth Amendment rules that have been designed to level imbalanced, one-sided tilts in the playing field, but does not do a good job explaining what courts have done with dual-assistance technologies that aid both the police and criminals. Almost all technologies that enable new forms of private surveillance qualify as dual-assistance technologies; the telephone system, for example, helps criminals develop conspiracies outside the public sphere, but it also helps the police, by generating a detailed record of spoken conversations. Because private surveillance will soon become the most important source of information for law enforcement, Kerr's theory suffers from a serious shortcoming that needs repair.

---

[4] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

The problems with Kerr's theory are its informality and indeterminacy. Essentially, it asks judges to determine which side of the crime-fighting equation benefits more from a given technology by performing an informal accounting of the benefits and burdens to each side. To lend rigor to this approach, I recommend that judges look for hard, objective measures of how much the playing field has tilted—statistical quantities like length of investigation and number of indictments. When criminals use new private services and technologies in ways that, for example, increase the average length of police investigations, judges should relax Fourth Amendment burdens on the police. Conversely, when the police use tools to decrease the average length of investigations, judges should tighten these burdens.

This Article proceeds in three parts. Part I predicts the rise of the surveillance society and focuses, in particular, on four recent innovations: the "one device," the cloud, the social, and "Big Data." Part II explains why traditional approaches to the Fourth Amendment might give rise to a surveillance state and reviews the critiques made by others of this traditional doctrine. Finally, Part III offers a new vision for the Fourth Amendment that is designed to survive the rise of the surveillance society.

I. THE DEATH OF PRIVACY

The past decade has seen the rise of a pervasive surveillance society not that different from the one famously anticipated in 1998 by David Brin in *The Transparent Society*.[5] Brin, a noted science fiction author writing a nonfiction book, predicted a future world in which cameras peer from every street corner, wasp-sized, pilotless drones enter our bedrooms, and companies compile massive databases tracking the purchases of every consumer.[6] Today, this description sounds like a fairly conventional and entirely plausible prediction of the near future, far less extraordinary than it seemed when written.

More recently, another fiction writer, Gary Shteyngart, anticipated an equally bleak near future—but one updated to reflect an

---

[5] DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998).

[6] *Id.* at 3-8.

additional decade of technological innovation—in his novel *Super Sad True Love Story*.[7] In Shteyngart's dystopia, the lives of the (mostly young) New Yorkers focus on their "äppärät"; handheld devices recognizable as the offspring of today's smartphones, but smaller and sleeker, which buzz with information and constantly stream information out to the world. Not only does this make every person the potential host of a live-streaming television show about his or her life, but also it makes every social interaction an opportunity for awkward self-revelation by telling each person who walks into a bar, for example, who does (and does not) want to sleep with him, and how highly he ranks in the crowd in categories like "hotness" and "personality."[8]

The truth is not far from the writings of these fiction writers. From among dozens of technological trends that are spurring these developments, let me focus on four: a tool, a piece of architecture, a new consumer motivation, and a class of techniques.

A. The One Device

First, consider the rise of the "one device," the convergence of a person's computing needs into a single, portable, high-powered machine, equipped with an always-on, high-speed connection to the Internet, and outfitted with dozens of sensors, including multiple digital cameras (capable of capturing still or moving images), a microphone, a GPS chip, and a digital compass.[9] Shteyngart's "äppärät" this is not, but it is close. This device knows where you are, who you are with, and what you are doing, saying, and looking at. It also sends all of this information to providers online. Today we call these devices the iPhone, iPad, and Android phone, but tomorrow they will have new names and new capabilities.

The one device enables new forms of private surveillance by giving people new modes of communication. As an already dated example, consider the text message. By giving people the ability to send short messages between phones, these devices have nearly

---

[7] GARY SHTEYNGART, SUPER SAD TRUE LOVE STORY: A NOVEL (2010).

[8] *Id.* at 90.

[9] Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 624 (2011).

obsoleted the short phone call and passed note.[10] Students gossip in class; spouses trade grocery lists; and employers (and drug lords) direct underlings using this relatively new medium. But as is true for all of the new technologies described in this Part, the replacement listens more and stores more than what it has replaced. Unlike the way telephone companies handle voice phone calls, text-messaging systems store copies of what is said on each endpoint and on network servers in the middle, too.[11] The one device coaxes us to communicate through it, and creates archives of what we say by default.

B. The Cloud

Second, and closely related to the one device, is the "cloud," the migration of essential computing and storage facilities from local devices owned by users to distant servers owned by providers.[12] Companies have recognized the benefits of development, deployment, and control that come from letting users access their calendars, word-processing documents, and stored files online.

Like text messaging and the one device, the cloud opens new avenues for surveillance—consider electronic mail. Before the rise of cloud-based e-mail, people tended to use e-mail accounts provided by their employers or ISPs, and they tended to download all of their messages periodically to their personal computers, leaving no copies behind on third-party servers. With the rise of Yahoo! Mail and Hotmail in the early part of the last decade, and Gmail a few years later, millions of users now store all of their messages with third parties.[13]

---

[10] *See* PEW INTERNET & AMERICAN LIFE PROJECT, TEENS AND MOBILE PHONES (Apr. 20, 2010), *available at* http://pewinternet.org/~/media//Files/Reports/2010/PIP-Teens-and-Mobile-2010-with-topline.pdf ("Fully two-thirds of teen texters say they are more likely to use their cell phones to text their friends than talk to them by cell phone.").

[11] *See* Jacob Leibenluft, *Do Text Messages Live Forever? How a Dirty SMS Can Come Back to Haunt You*, SLATE (May 1, 2008, 6:51 PM), http://www.slate.com/id/2190382/.

[12] 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) (describing cloud computing).

[13] PEW INTERNET & AMERICAN LIFE PROJECT, USE OF CLOUD COMPUTING APPLICATIONS AND SERVICES (Sept. 2008), *available at* http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf (reporting that fifty-six percent

A more recent shift to the cloud has been the rise of services, like Google Docs, that provide word processing and spreadsheet handling in the cloud.[14] Before Google Docs, almost nobody systematically stored all their writings with a third party, but now some people do, and more join their ranks each week. This shift may prove even more important than the shift to cloud-based e-mail, because it exposes not only communications, but also accounting workbooks, contracts, and formal correspondence to surveillance.

C. The Social

Technical advances like smartphones and the cloud mean little if consumers choose not to adopt them. The rise of what I call "the social" has given them a reason to do so. Today's social networks—most importantly Facebook but also Twitter, Google+, and services from related companies like Zynga—build upon the innate desire of humans to want to connect to others. Software developers have realized that the simple act of allowing people to see what others are doing can trigger psychological feelings of trust and entertainment.

Once again, the rise of the social can be viewed as a boon to private surveillance. On social networks, people reveal more of their thoughts and behavior, including things they might have before chosen to hide, and to more people than they ever have before. And as with everything else that has been discussed, social networking technologies almost always store copies of all these revealed facts.

D. Big Data

The last crucial development is the rise of what some have termed Big Data, the use by companies of powerful new data analytics that help companies squeeze more value from their existing data by making inferences.[15] I have investigated some of

---

of American Internet users "use webmail services such as Hotmail, Gmail, or Yahoo! mail").

[14] *Id.* (reporting that twenty-nine percent of American Internet users "[u]se online applications such as Google Documents or Adobe Photoshop Express").

[15] *See New Rules for Big Data: Regulators are Having to Rethink Their Brief*, ECONOMIST (Feb. 25, 2010), http://www.economist.com/node/15557487; *see also* Danah

the power of Big Data in my work on reidentification.[16] To the surprise of many, computer scientists have demonstrated that they can often take a database full of anonymized data—data in which things like names, social security numbers, and photos have been intentionally removed to protect privacy—and restore identity by studying patterns in the data.[17] Big Data will have a profound impact on privacy, one which is still being explored by legal scholars.[18]

Big Data promises to have the biggest impact of all on law enforcement. Soon, the third parties that already hold information about us will be able to infer private details about our lives, even things we intentionally withhold from them. Students in a class at M.I.T. claimed they could determine the sexual orientation of anonymous users based only on the patterns with which they friend others on Facebook.[19] Others have used off-the-shelf facial recognition software to connect photos taken on a cheap consumer web camera to user profiles on Facebook and a dating website.[20] Worse yet, they used the information they learned from Facebook to guess the first five digits of the person's social security number with reasonable success, building a simple pathway from a quick glimpse of a person in public to potential identity theft.[21]

This is just the beginning. As terrifying as these examples of Big Data seem to be, they still bear some connection to rational explanation. The worst will come when we throw rationality out the window and people begin to draw inferences that defy rational explanation and that reveal true facts about individuals that the

---

Boyd, *Privacy and Publicity in the Context of Big Data*, DANAH (Apr. 29, 2010), http://www.danah.org/papers/talks/2010/WWW2010.html.

[16] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

[17] *Id.* at 1703-04.

[18] *Id.*; Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011).

[19] Nadia Wynter, *'Gaydar' Project at MIT Attempts to Predict Sexuality Based on Facebook Profiles*, N.Y. DAILY NEWS, Sept. 22, 2009, at A1, *available at* http://articles.nydailynews.com/2009-09-22/entertainment/17932462_1_gay-sexuality-facebook ("Gay men had proportionally more gay friends than straight men, giving the computer program a way to infer a person's sexuality based on their friends.").

[20] Alessandro Acquisti et al., Presentation at BackHat 2011: Faces of Facebook: Privacy in the Age of Augmented Reality (Aug. 4, 2011), *available at* https://www.blackhat.com/docs/webcast/acquisti-face-BH-Webinar-2012-out.pdf.

[21] *Id.*

subjects may not even realize about themselves.[22] We are embarking on the age of the impossible-to-understand reason, when marketers will know which style of shoe to advertise to us online based on the type of fruit we most often eat for breakfast, or when the police know which group in a public park is most likely to do mischief based on the way they do their hair or how far from one another they walk.

E. The Surveillance Society

These four trends, taken together, enable the rise of a powerful, new surveillance society, one which raises significant new threats to privacy. To understand more fully what I mean by a new surveillance society, consider what happens when you combine the four advances—the one device, the cloud, the social, and Big Data—to enable an application that has been often in the news lately: location tracking.[23]

Before we consider the way the police can track our location today, think about how they tracked location in the past with a tracking beeper, an expensive, complex device that federal agencies expended great amounts of money to develop. These devices had to be long-lived, small enough to hide, yet big enough to hold large batteries.[24] To install these devices, the police had to risk discovery by sneaking onto a private driveway or into a parking garage.

Today, the use of a tracking beeper seems to be an unnecessary law enforcement risk, because almost every one of us voluntarily carries a personal tracking beeper. When switched on, mobile phones periodically ping the airwaves, looking for cell

---

[22] *E.g.*, Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES, Feb. 19, 2012, at MM30 (describing use by Target of data analytics to identify pregnant potential shoppers).

[23] *See* Janice Y. Tsai et al., *Location-Sharing Technologies: Privacy Risks and Controls*, 6 I/S: J.L. & POL'Y INFO. SOC'Y 119 (2010); Strandburg, *supra* note 9, at 631-33 (discussing location tracking and the Fourth Amendment).

[24] Kim Zetter, *Caught Spying on Student, FBI Demands GPS Tracker Back*, THREAT LEVEL—PRIVACY, CRIME AND SECURITY ONLINE, WIRED (Oct. 7, 2010, 10:13 PM), http://www.wired.com/threatlevel/2010/10/fbi-tracking-device/ (quoting an unnamed former FBI agent explaining that newer tracking devices are hardwired to the tracked car's battery, obviating the need for its own power source). In 2010, two different people discovered these devices strapped to their cars and shared them with the press. *Id.*; *FBI Tracking Device Teardown*, IFIXIT BLOG (May 9, 2011), http://www.ifixit.com/blog/blog/2011/05/09/fbi-tracking-device-teardown/.

towers in close proximity.[25] Cell phone providers track these registrations to help route calls and monitor the health of their networks. But through a technique known as trilateration, one can take the record of cell tower usage and locate a person with great accuracy, even with "a level of accuracy that can approach that of GPS."[26]

And, thanks to the rise of the smartphone, the FBI's ability to track cell phones increases every year. These phones almost always include a GPS chip and a digital compass (to indicate the direction the user is facing) and come loaded with software packages that coax the user to reveal his location to third-party services.[27] Even three years ago, private companies rarely cared where its online users sat on the globe except at the level of granularity of the nation, state, or province.[28] Today, location-based services are widely deployed and spreading quickly. Services like Loopt[29] and Foursquare[30] try to overlay social networks atop the physical grid, creating a new sport of "checking-in" to stores and restaurants. This is all fueled by new advertising models, and many companies in Silicon Valley are racing to squeeze the untapped dollars available to those who can market locally, viewing Groupon's success in this space with envy.[31]

---

[25] Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES, Mar. 26, 2011, at A1, *available at* http://www.nytimes.com/2011/03/26/business/media/26privacy.html ("[W]e are already continually being tracked whether we volunteer to be or not.").

[26] *ECPA Reform and the Revolution in Location Based Techonologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 112th Cong. 1, 10 (2010) (testimony of Professor Matt Blaze), *available at* http://www.crypto.com/papers/blaze-judiciary-20100624.pdf. Professor Matt Blaze described "'network based' location techniques [that] can give the position of virtually every handset active in the network at all times." *Id.* at 6.

[27] Jordan Robertson, *Your Phone, Yourself: When is tracking too much?*, USA TODAY (Apr. 23, 2011, 10:39 PM), http://www.usatoday.com/tech/news/2011-04-23-smartphone-tracking.htm.

[28] *See generally* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD (2006).

[29] LOOPT.COM, https://www.loopt.com/ (last visited Feb. 21, 2012).

[30] FOURSQUARE.COM, https://foursquare.com/ (last visited Feb. 21, 2012).

[31] James Surowiecki, *Groupon Clipping*, NEW YORKER (Dec. 20, 2010), http://www.newyorker.com/talk/financial/2010/12/20/101220ta_talk_surowiecki ("The market for local advertising, which is really the business Groupon is in, is huge (more than $130 billion a year) and still relatively untapped online."); *see also* Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, WALL ST. J. (Dec. 17, 2010, 10:01

Of course, the disintegration of privacy to the commercial sector is an old trend that has been remarked upon for years. Even so, these four relatively new advances—the one device, the cloud, the social, and Big Data—mark an acceleration of the trend. We have turned a corner in the graph of power/invasiveness over time. Thanks to the increasing power of portable devices and their emphasis on location awareness, the rise of the cloud, and the power of Big Data, the power, extent, sophistication, and interrelatedness of private systems of surveillance are increasing at rates that suggest a difference in kind not just degree.

II. THE DIMINISHED FOURTH AMENDMENT

While some legal scholars have argued that we abandon the reasonable expectation of privacy test, and still others have anchored the Fourth Amendment in principles other than privacy, none of these scholars has considered the central question of this Article: what if we are headed for a world without privacy? This shift in focus gives a different, more urgent impetus to some of the prescriptions that others have offered, but it also gives rise to the need for new prescriptions.

In a world without privacy, a Fourth Amendment focused on privacy becomes nearly a dead letter. Today's Fourth Amendment has been built around the reasonable expectation of privacy test, but no expectation of privacy will be deemed reasonable in a world without privacy. Even worse, the great bulwark of the Fourth Amendment, probable cause and a warrant, will become much less important as pervasive monitoring and record collection will give the police probable cause most of the time.

The diminishment of the Fourth Amendment will change police behavior. Police agencies will begin to abdicate their traditional role as conductor of surveillance, because it will be eclipsed by the powerful new systems of private surveillance. The FBI and other law enforcement agencies will shift from being active producers of surveillance to passive consumers, essentially outsourcing all of their surveillance activities to private third parties, ones

---

PM), http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html ("[A]ds targeted by location bring in two to five times as much money as untargeted ads.").

who are not only ungoverned by the state action requirements of the Fourth Amendment, but also who have honed the ability to convince private citizens to agree to be watched.

It is likely, however, that courts will resist this change, refusing to accept a nugatory Fourth Amendment. To save the Fourth Amendment, they will transform it, abandoning the reasonable expectation of privacy test. To replace it, courts may turn to legal scholarship, which to date has failed to fully elaborate what should come next.

A. The End of Self-Help Policing

Before examining what the rise of the surveillance society means for the Fourth Amendment, consider what it means for the practicalities of policing. We should expect a major shift in the center of activity of crime fighting from the police to private industry. The surveillance society will greatly diminish the importance of self-help policing.

In constitutional criminal procedure, the difference between self-help policing and assisted policing has received little attention, because almost all court attention has focused on the former. In the near century since *Olmstead*,[32] almost all of the cases discussing what new technology means for the Fourth Amendment have involved police self-help and home-grown tools. The police inserted the wires into the telephone lines in *Olmstead*,[33] mounted the recording device in *Katz*,[34] deployed its own microphones in *Goldman*[35] and *Silverman*,[36] chartered aircraft for their own use in *Ciraolo*[37] and *Dow Chemical*,[38] and installed their own tracking beepers in *Karo*[39] and *Knotts*.[40] Future students of the amendment are likely to marvel at these historical relics, trying to imagine a time when the FBI was forced to build its own tools and collect its own data. It will likely seem a far cry from the FBI they

---

[32] Olmstead v. United States, 277 U.S. 438 (1928).
[33] *Id.* at 457.
[34] Katz v. United States, 389 U.S. 347, 348 (1967).
[35] Goldman v. United States, 316 U.S. 129, 131 (1942).
[36] Silverman v. United States, 365 U.S. 505, 506 (1961).
[37] California v. Ciraolo, 476 U.S. 207, 209 (1986).
[38] Dow Chem. Co. v. United States, 476 U.S. 227, 229 (1986).
[39] United States v. Karo, 468 U.S. 705, 708 (1984).
[40] United States v. Knotts, 460 U.S. 276, 277 (1983).

know: agents sitting in offices, acting as a central clearing house for the observations of private industry, mining their way through mountains of data collected by other people and for other purposes.

It is as if today's FBI has developed a sophisticated surveillance research-and-development arm with field offices named Apple, Google, Facebook, Comcast, and AT&T.[41] 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 these labs 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.[42]

Although few scholars have noted what the end of self-help policing means for the Fourth Amendment, some have noted the descriptive shift in the amount the police and intelligence community rely on the fruits of private surveillance. Jon Michaels has carefully tracked the increasing reliance on technological advances and private surveillance by the intelligence community.[43] Others have noted how much the CIA, FBI, and Defense Department rely on the services of data aggregators like ChoicePoint.[44]

As proof of the shift away from a self-help police force, consider the annual Wiretap Report. By statute, the Administrative Office of the United States Courts is charged with issuing a report each year that tallies the number of applications for court-ordered wiretaps in state and federal court and requires a small number of summary statistics about each jurisdiction.[45]

---

[41] *See* David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165, 1177 (1999) (discussing "out-contracting, in which government agencies hire private security companies to perform work previously carried out by law enforcement officers," at the time, a rapidly growing practice).

[42] *See* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 908 (2008) ("People simply do not interface with the government in the same ways or with the same frequency as they do with the private sector, and thus the intelligence agencies find themselves particularly drawn to, and in some respects dependent upon, private data resources.").

[43] *Id.* at 901-66.

[44] Joshua L. Simmons, Note, *Buying You: The Government's Use of Fourth-Parties to Launder Data about "The People,"* 2009 COLUM. BUS. L. REV. 950, 994 (2009).

[45] 18 U.S.C. § 2519 (2006).

One table of the report breaks down wiretap orders by the "type of surveillance used," oral (voice), wire (telephone), electronic (computer network).[46] Some have expressed surprise, even suspicion, at the low number of electronic orders granted every year. For example, in calendar year 2010, out of 2,311 wiretaps ordered nationwide, only sixteen involved electronic surveillance (defined as "Digital Pager, Fax, and Computer"), or approximately 0.7%.[47] This is not an outlier, as indicated by Figure 1, which plots both the total number and percentage of all wiretaps that involved electronic surveillance for the past fifteen years.

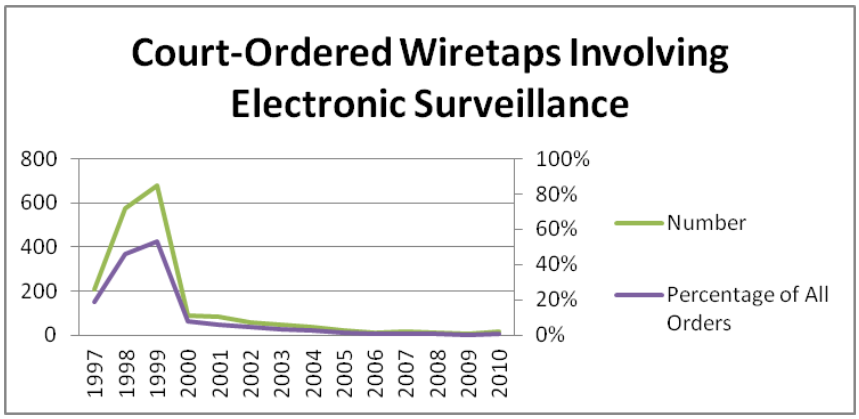

Figure 1: Court-Ordered Wiretaps Involving Digital Evidence (1997-2010)[48]

Figure 1 provides a compelling visual image of the decline of self-help policing. Clearly, the number of court ordered wiretaps involving electronic evidence dropped precipitously at the turn of the century. Chris Soghoian, a close watcher of these statistics,

---

[46] *See, e.g.*, DIR. OF THE ADMIN. OFFICE OF THE U.S. COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 27 tbl.6 (June 2011), *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2010/Table6.pdf.

[47] *Id.*

[48] Figure 1 was constructed using data from the 1997 through 2010 *Wiretap Reports* issued by the Director of the Administrative Office of the United States Courts. For the detailed data see *Wiretap Reports*, UNITED STATES COURTS, http://www.uscourts.gov/Statistics/WiretapReports.aspx (follow "Wiretap Report YEAR" hyperlink for each yearly report; then follow "Table 6" hyperlink) (last visited Feb. 21, 2012).

speculates that this is proof of the declining importance of fax transmissions in criminal surveillance, which are included in this reporting category.[49] But the drop since 2000 is nearly as pronounced, with a near linear decline from 2000 (eighty-nine intercepts, nearly eight percent of all)[50] to 2006 (thirteen intercepts, 0.76%).[51] Since 2006, the nation's courts have authorized fewer than twenty wiretaps of digital networks a year, never topping one percent of all orders in that time span.[52]

The dramatic decrease is almost certainly not an indication that criminals use computer networks less or that the police rely less on network surveillance. Instead, it likely represents a shift in police tactics away from self-help. Today, it makes little sense for the police to engage in court-ordered wiretapping. Not only is it easier to secure private cooperation than judicial sanction, but also the fruits of private surveillance are simply better—fed as

---

[49] Christopher Soghoian, *8 Million Reasons for Real Surveillance Oversight*, SLIGHT PARANOIA BLOG (Dec. 1, 2009, 7:00 AM), http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html ("I suspect that the nearly 700 electronic intercept orders granted in 1998 were largely for fax machines and pagers. Thus, as these technologies died out, it is only natural that the number of electronic intercept orders declined[.]").

[50] DIR. OF THE ADMIN. OFFICE OF THE U.S. COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 27 tbl.6 (Apr. 2001), *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2000/table600.pdf.

[51] DIR. OF THE ADMIN. OFFICE OF THE U.S. COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 27 tbl.6 (Apr. 2007), *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2006/Table62006.pdf.

[52] The Wiretap Reports indicate also the number of "Combination" wiretaps, which "refers to installed intercepts for which more than one type of surveillance was used." DIR. OF THE ADMIN. OFFICE OF THE U.S. COURTS, *supra* note 46. Since there are only three types of surveillance that might be joined in combination—oral, wire, and electronic—the odds are that some of the combination wiretaps involve electronic surveillance. Even if we assume that all combination wiretaps involve electronic surveillance—an unlikely possibility—the addition of these numbers does not change the trend substantially. To take one representative year, in 2008, out of 1809 wiretaps, ten were classified as involving electronic surveillance and thirty-three were combination, increasing the percentage from 0.55% to 2.38% of all wiretaps. DIR. OF THE ADMIN. OFFICE OF THE U.S. COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 27 tbl.6 (Apr. 2009), *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2008/Table6.pdf

they are by our sensor-laden world and empowered by consensual sharing.

Figure 1 is a bellwether not an outlier. With each passing year, the police will learn to borrow and beg rather than build. Our mental image of the FBI agent conducting surveillance, wearing headphones in a white van parked on the curb, clipping alligator clips to telephone wires, and working with a white-coated FBI scientist will soon be replaced by an agent sitting in his office, hitting the refresh button on his web browser, and reading the latest log file dump sent from private industry.

Consider one final example. In the late 1990s, the FBI faced a firestorm surrounding its Carnivore system—a piece of software developed in-house and designed to perform electronic wiretapping on digital networks—in technical terms, a filtering packet sniffer.[53] The public story is well known: the press dug deep, the public complained, and Congress raged, ultimately passing laws requiring better reporting about the FBI's use of the system.[54] The less-well-known denouement is also telling: a few years after the controversy, the FBI abandoned Carnivore's successor, realizing that the private computer security industry had designed better filtering packet sniffers than the FBI could do on its own.[55] This shift is a herald of the shift in role and responsibility for surveillance from FBI labs to private companies, which we will see repeated constantly in the years to come.

B. No More Expectations of Privacy

In *Katz*, the Supreme Court embraced a new doctrine of the Fourth Amendment built on privacy. This took the form of the majority's pronouncement that "the Fourth Amendment protects people, not places,"[56] and Justice Harlan's "reasonable expectation of privacy" test in a concurring opinion,[57] which was later embraced by the Court as the test for the meaning of search within

---

[53] Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 648-54 (2003).

[54] *Id.* at 654-58.

[55] Ted Bridis, *FBI Abandons its Software for Online Wiretaps, Bureau Switching to Commercial Snooping System*, CHI. TRIB., Jan. 19, 2005, at 12.

[56] Katz v. United States, 389 U.S. 347, 351 (1967).

[57] *Id.* at 360-61 (Harlan, J., concurring).

the amendment.[58] Although the rest of this Part will examine in-depth what happens to a privacy-centric Fourth Amendment in a world without privacy, the punch line is both easy to state and preordained almost to the point of being tautological—in a world without privacy, a Fourth Amendment built around reasonable expectations of privacy will no longer apply.

Specifically, the courts have given the reasonable expectation of privacy test three additional elaborations, and each suggests that when courts face fact patterns arising from the rise of the surveillance society, they might hold that the Fourth Amendment does not apply.

1. Assumption of Risk

According to the Supreme Court, an individual

> takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . [E]ven if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[59]

This reasoning has been applied in at least two important and broad contexts, which are both implicated by the surveillance society: the false friends rule and the third-party doctrine. Under the false friends rule, exemplified by cases like *Hoffa v. United States*,[60] we share secrets with other people at our own risk, and if the people we think are trusted confidants turn out instead to be government agents wearing a wire, we have only ourselves to blame, and the Constitution provides no relief.[61]

The reasoning has extended not only to friends but also to the companies we use for essential services. The Supreme Court has declared that the Fourth Amendment does not apply to our bank's

---

[58] Smith v. Maryland, 442 U.S. 735, 740 (1979).
[59] United States v. Miller, 425 U.S. 435, 443 (1976).
[60] 385 U.S. 293 (1966).
[61] *Id.* at 302.

records of our financial transactions,[62] or to our phone company's lists of numbers we have dialed.[63]

Notice how this rule automatically expands police power to some of the new forms of private surveillance. Consider for example the location records people now share regularly with Loopt[64] and Foursquare.[65] Because we share our location consensually with companies like these, courts are likely to treat this information as constitutionally unprotected under the reasoning of the assumption of risk cases.

2. Knowing Exposure

Under the knowing exposure rule, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[66] The Supreme Court has used this reasoning to rule that the police can track a car with an electronic beeper as it moves around city streets, because the car remains on public thoroughfares.[67] It has also used the concept of knowing exposure to deem outside the Fourth Amendment the use by the police of airplanes and helicopters to look at the open fields and even the curtilage next to a person's home.[68]

Knowing exposure means that some of the information shared online through private services may be accessed by the police, because new online services obscure the already blurry line between what we treat as private and public. Consider for example what you say on your Facebook account. Is a Facebook account a public or private space? Does it depend on the number of friends you have or the configuration of your privacy settings? Complicating this considerably is Facebook's ongoing war with its users about those privacy settings and, in particular, what the default settings should be. A court could reasonably hold that some of the content posted to Facebook has been knowingly exposed to the

---

[62] *Miller*, 425 U.S. at 442-43.

[63] *Smith*, 442 U.S. at 744-45.

[64] LOOPT.COM, *supra* note 29.

[65] FOURSQUARE.COM, *supra* note 30.

[66] Katz v. United States, 389 U.S. 347, 351 (1967).

[67] United States v. Knotts, 460 U.S. 276, 282 (1983).

[68] Dow Chem. Co. v. United States, 476 U.S. 227, 238-39 (1986); California v. Ciraolo, 476 U.S. 207, 214-15 (1986).

public and, following conventional Fourth Amendment law, rule that it may be obtained by the police without a warrant.

3. General Public Use

Finally, the general public use rule comes from two cases, *Dow Chemical*[69] and *Kyllo*.[70] According to this rule, the police may deploy powerful surveillance devices to track suspects without a warrant so long as the tool is generally accessible to the public. In *Dow Chemical*, the court held that a $22,000 camera qualified under this rule.[71] Although the Court backtracked a bit in *Kyllo*, finding a $1000 thermal heat-imaging machine did not qualify as one in general public use, it refused to overrule *Dow Chemical*.[72]

As the power of private surveillance increases, the devices and systems they create may be available to the police without process because of this rule. Consider for example powerful reidentification techniques. Some day, private companies may develop a tool to convert the supposedly anonymous comments on a public message board into the commenter's true identity by cross-referencing the attributes of the communication with rich outside databases using powerful reidentification techniques.[73] Whether the police could use technology like this without a warrant may turn on the general public use test, which means a warrant may not be needed once reidentification tools become cheap and widespread.

Because of these three rules, the systems of private surveillance I sketched in Part I may become, by default and in lockstep, a system of public surveillance. The coming surveillance system could give rise to a powerful, pervasive surveillance state, at least if traditional approaches to the Fourth Amendment apply. With each passing year, the police might find that their power grows with every industry product launch. The people would be watched

---

[69] 476 U.S. at 227.

[70] Kyllo v. United States, 533 U.S. 27 (2001).

[71] 476 U.S. at 238.

[72] *Kyllo*, 533 U.S. at 39 n.6.

[73] *Cf.* Farkhund Iqbal et al., *A Novel Approach of Mining Write-Prints for Authorship Attribution in E-Mail Forensics*, 5 DIGITAL INVESTIGATION 42-51 (2008), *available at* http://www.dfrws.org/2008/proceedings/p42-iqbal.pdf (describing statistical techniques that can identify authors of anonymous writings).

in ways that they would not have been; records of their behavior would be created and retained when once they would have been never created or destroyed; and traditional forms of surveillance would occur much more thoroughly and efficiently than they have before.

C. The Inevitable Search for the New Fourth Amendment

It is possible that courts will follow the doctrinal path sketched above, issuing a series of opinions that render the Fourth Amendment a dead letter. Perhaps the Fourth Amendment will fade into the dustbin of history, following the Third Amendment's right against state mandated quartering of soldiers as another idea 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. They might see changing social norms spurred by shifting technological possibilities as a fundamental shift in the foundation upon which the original Framers built, a reason to redefine reasonableness, search, and seizure.

But it seems unlikely that courts will take this particular path. Courts seem unlikely to abandon one of the principle limitations of state power in our founding document, an amendment that Akhil Amar argues "literally and in every other way, belongs at the center of the Bill of Rights."[74] This is true regardless of the political priors of judges considering the question and the method of constitutional interpretation he or she embraces. Originalists and textualists will argue that the amendment was never really about privacy at all. Living constitutionalists will find within the open texture of the amendment's language the freedom to shape the concept of unreasonable search and seizure to changed circumstances.

The result will be a concerted effort to find new underpinnings for a new interpretative theory and jurisprudence of the Fourth Amendment. Unfortunately, the judges engaged in this

---

[74] Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 811 (1994).

effort will find very little concrete guidance in legal scholarship, because even though many scholars have grumbled about the amendment's shortcomings, the answers they have offered are inchoate, only partially defined, and ultimately not nearly enough to provide a way forward.

D. Other Solutions and Their Limits

Today, few legal scholars speak in favor of *Katz* and the reasonable expectation of privacy test, and even fewer can muster anything kind to say about the third-party doctrine.[75] One would expect, therefore, to find answers in the prescriptive approaches that they have presented. Although some of these scholars have discovered useful frameworks pointing to what comes next, none has yet come close to offering the judges who will soon abandon reasonable expectations of privacy a detailed and concrete way forward.

Some authors have proposed abandoning the third-party doctrine.[76] Others have advocated a redefined Fourth Amendment that focuses on power instead of privacy.[77] Still others have recommended viewing the Fourth Amendment as a question of policy rather than mere expectations.[78] These writers offer useful starting points, but none comes close to offering a fully realized theory. Some offer abstract prescriptions that are too difficult to translate into useful, predictable rules. Others offer solutions that are more concrete but unfortunately do not go far enough to restoring a meaningful role for the Fourth Amendment.

One reason why none of these authors has gone far enough may be because none has been willing to follow the conceit of this Article—that privacy may soon vanish from this country. These authors have all recognized, to greater or lesser extent, that privacy is on the decline or has rapidly been redefined, but these middle-strength observations and predictions have given rise to proportionate half measures. But if privacy is almost a dead letter, and if the end of it will come soon, then the limits of these past prescriptions are clear.

---

[75] *But see* Kerr, *supra* note 3 (offering a defense of the third-party doctrine).

[76] *See infra* Part II.D.1.

[77] *See infra* Part II.D.3.

[78] *See infra* Part II.D.2.

1. Why Abandoning the Third-Party Doctrine Isn't Enough

The standard move made by legal scholars in articles like this is to focus on the third-party doctrine—the rule that states:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[79]

Or, more concisely, "[b]y disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed."[80]

Some critics contend that the third-party rule is a mistake in every context and should be overturned.[81] Others would restrict it to its original contexts—bank records and telephone numbers dialed—but prevent it from spreading to other network services like electronic mail, cloud computing, and mobile location.[82] What remains consistent throughout this literature is the idea that the third-party doctrine deserves to be our central focus, that if only we could rein it in, we could right the balance between police power and privacy. Fixing the third-party doctrine, in short, is both necessary and sufficient to fixing the problem of police surveillance of private behavior.

In a world without privacy, however, getting rid of the third-party doctrine is necessary but not nearly sufficient to ensure the appropriate protection of the Fourth Amendment. The third-party

---

[79] United States v. Miller, 425 U.S. 435, 443 (1976).

[80] Kerr, *supra* note 3, at 563.

[81] Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 265 (2006).

[82] Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1407 (2004) ("[T]he argument that, under *Miller*, the mere fact that a subscriber places his or her communications with a third-party service provider eliminates any expectation of privacy in those communications is doctrinally and normatively unsound."); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 41, *available at* http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf ("The analogy between banking records and stored e-mails does not hold."); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1578 (2004).

doctrine and, more broadly, the Fourth Amendment have traditionally evolved to focus attention almost entirely on the requirement that a search warrant be issued only with probable cause and particularity.

In a world without privacy, probable cause and a warrant by themselves will not do enough to give effect to the full protection of the amendment. Although judges will be able to squelch fishing expeditions, fishing expeditions will no longer be necessary.[83] This is the power of a widespread surveillance society. It produces interconnected databases that track the behavior of millions in excruciating detail, gives companies (and the police agencies they assist) detailed records of what every one has done, and produces chains of evidence that can connect criminals to crime with no breaks and no ambiguous midway points.[84]

The result is that even if we increase probable cause and warrant requirements, we still will be subject to far too much arbitrary surveillance. If the police are tracking a person knowing only the time and place of the crime and a general description of the perpetrator, they will be able to access cell phone location databases or video surveillance log files (with probable cause) to make the match. If they know that a particular e-mail address was used, then they will be able to search the login databases for the e-mail provider.

Reversing or narrowing the third-party doctrine will help stem official arbitrariness, but it will not do enough to reverse the unprecedented increase in police power that the surveillance society has created. The problem with the surveillance society is not simply how it empowers the bored police officer on a fishing expedition; it is a broader problem with an increase in the power of the state to watch, listen, and follow every one of us.

2. The Limits of Policy

Many scholars dissatisfied with the evolution of the reasonable expectation of privacy test since *Katz* recommend that judges replace it or implement it using a first-principles, free-wheeling,

---

[83] Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514, 1544 (2010).

[84] *Id.* at 1530-32. *See also infra* Part III.D.

normative style of analysis. They take as both their inspirational model and precedential green light Justice Harlan, who not only invented the reasonable expectation of privacy test in his *Katz* concurrence, but also shortly thereafter tried (in dissent) to modify it to embrace this kind of naked, normative mode of analysis.[85] Justice Harlan argued:

> Since it is the task of the law to form and project, as well as mirror and reflect, we should not, as judges, merely recite the expectations and risks without examining the desirability of saddling them upon society. The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens, the risks of the electronic listener or observer without at least the protection of a warrant requirement.[86]

Justice Harlan explained further that he was proposing a balancing test of "assessing the nature of a particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement."[87]

As we search for a replacement for reasonable expectation of privacy, Justice Harlan provides a potential starting point, but not more than that. The problem with the purely normative inquiry is its imprecision and variability. A test that explores solely "the desirability of saddling [particular practices] upon society"[88] is a non-test, which invites little more than rules based on the prior predilections of each judge. Even worse, such a starting point will lead to complete unpredictability, at least to start, which will leave police officers incapable of knowing what to do in most situations, particularly those involving new, untested waters. Given

---

[85] *See, e.g.*, Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *is Made Of?*, 41 U.C. DAVIS L. REV. 781, 795 (2008) (discussing the "'is-ought' problem" of the reasonable requirement); Catherine Hancock, *Warrants for Wearing a Wire: Fourth Amendment Privacy and Justice Harlan's Dissent in* United States v. White, 79 MISS. L.J. 35, 35 (2009); Freiwald, *supra* note 82, ¶¶ 30-31 (discussing the need for a "normative inquiry").

[86] United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

[87] *Id.*

[88] *Id.*

the severe sanction of the exclusionary rule, this kind of uncertainty is unacceptable.[89]

The other reason to be wary of a pure policy interpretation of the Fourth Amendment is the tendency for policy debates about privacy and security to end up one-sided. In his book, *Nothing to Hide*, Daniel Solove catalogs a number of distorting features of the debate between privacy and security that tend to push decision makers to privilege security.[90] For example, he discusses the common retort that privacy is needed only for those with something embarrassing or shameful they want to conceal—the nothing-to-hide argument[91]—or the fallacy that privacy and security are inversely proportional qualities locked in a zero-sum tournament—the all-or-nothing belief.[92]

3. From Privacy to Power

If the Fourth Amendment does not intrinsically promise privacy, what does it provide? Many scholars have argued that the Fourth Amendment should be interpreted as being about power, not just privacy. Some place this in an originalist frame. The colonists designed the amendment to respond to the Crown's use of general warrants, blanket authorities that entitled British troops to search people and homes (and "papers and effects") indiscriminately and without suspicion.[93] Although these indignities involved privacy harms, the more important problem seemed to be the way they defined their relationship with the state, a relationship marked by insecurity and imbalanced power.

Now that privacy is fading, we need to take the claims of these scholars more seriously if the Fourth Amendment is to survive. The end of privacy disrupts the rules we use to give action to the amendment, and we must shift away from *Katz*'s reasonable

---

[89] Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 527 (2007) ("The Fourth Amendment's suppression remedy . . . generates tremendous pressure on the courts to implement the Fourth Amendment using clear ex ante rules rather than vague ex post standards.").

[90] DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011).

[91] *Id.* at 21-32.

[92] *Id.* at 33-37.

[93] Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 296-97 (1993).

expectation of privacy to rules that focus instead on the balance of power between the police and the people.

In his book, *Nothing to Hide*, Dan Solove recommends that we abandon the reasonable expectation of privacy test, because it is "not focused on the right question."[94] This is because "[i]n many instances, what is or isn't protected by the Fourth Amendment bears no relation to the problems caused by government information gathering"—namely, "whether it is best to have judicial oversight of law enforcement activity, what that oversight should consist of, how much limitation we want to impose on various government activities, and how we should guard against abuses of power."[95]

Law professor Thomas Clancy has sounded a similar theme in urging courts and legal scholars to conceptualize the Fourth Amendment as not only about privacy and property but also "security from unreasonable governmental intrusion."[96] This interpretation of the amendment, which of course finds better textual support than "privacy,"[97] stemmed from the colonists' experience with the "arbitrary exercise of [British] power to invade their property."[98] "The Framers valued security and intimately associated it with the ability to exclude the government."[99] In similar terms, Jed Rubenfeld has argued that "[t]he Fourth Amendment does not guarantee a right of privacy. It guarantees—if its actual words mean anything—a right of *security*."[100]

Other scholars have made similar points. Morgan Cloud has argued that "[t]he text and history of the Fourth Amendment demonstrate that it exists to enhance individual liberty by constraining government power."[101] Bill Stuntz argued that the

---

[94] SOLOVE, *supra* note 90, at 114.

[95] *Id.* at 115.

[96] Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 351 (1998) (internal quotation marks omitted).

[97] *See* 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" (emphasis added)).

[98] Clancy, *supra* note 96, at 352.

[99] Clancy, *supra* note 96, at 353.

[100] Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 104 (2008).

[101] Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 618-19 (1996)*; see*

Fourth Amendment should focus not only on privacy, but also on "concern with coercion and violence."[102] Thomas Crocker finds that the Fourth Amendment does not adapt well to new forms of "social privacy," suggesting instead that it "should be refocused in light of the protections provided interpersonal liberty."[103]

III. THE FOURTH AMENDMENT'S THIRD ACT

A. Katz *is the New* Olmstead

In one hundred years, when we look back on the history of the Fourth Amendment, we will realize that for a long time we misunderstood the relationship between privacy and the amendment. We think of them today as intrinsically connected, but this is an illusion.

Privacy is simply a proxy for what the amendment protects. It is a proxy that served us well for a long time because technology and social practices have historically moved so slowly. But today, nothing seems to move as quickly as technology, and nothing in the text of the amendment explicitly depends on privacy or on a society that respects privacy. This may seem surprising, both because the Fourth Amendment has for so many decades focused on privacy, but also as a matter of textual analysis. The amendment's central focus on the word "search" suggests a natural connection to the concept of privacy.

But the age of using privacy as a measuring stick for Fourth Amendment protection is likely soon to draw to a close. Of course, a similarly radical shift has happened before. The earliest cases conceived of the Fourth Amendment as designed to protect property, with this view reaching its zenith in the *Olmstead* Court's refusal to extend the amendment to wiretapping because "[t]he language of the Amendment cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of

---

also Cloud, *supra* note 93, at 295 ("The fourth amendment exists for the very purpose of enhancing individual liberty by constraining government power.").

[102] William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 446 (1995).

[103] Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After* Lawrence, 57 UCLA L. REV. 1, 56 (2009).

his house or office any more than are the highways along which they are stretched."[104] Almost four decades later, this style of reasoning was entirely repudiated, and the foundation of the Fourth Amendment was swapped out completely, replaced by the reasonable expectation of privacy test.[105] The Fourth Amendment survived one fundamental shift; it is due for another.

And when the history of our current epoch—the Fourth Amendment's second act—is written, we will probably consider it a happy accident that our conceptions of privacy and power served one another so well for so long. As Thomas Crocker puts it:

> Fourth Amendment privacy and the liberty ordinarily protected under due process may overlap, and the former may be valued for its ability to foster the latter, but the two need not always coincide. Thus, if the Fourth Amendment is understood to protect liberty as well as privacy, new constitutional possibilities emerge for shielding interpersonal relations from state intrusion.[106]

Privacy, with all of its messy connotations and contextual variation, has seemed to map, more or less appropriately, with the balance of power we wanted vis-à-vis the state. It does no more, and we need to start over, again.

We will be eased in our task of abandoning the fundamental underpinning of the Fourth Amendment by learning lessons from the last time we did something similar. The most important lesson we can learn is that though today we look past property in elaborating the Fourth Amendment, we have never really abandoned it. Contrary to Justice Stewart's admonishment that the "Fourth Amendment protects people, not places,"[107] today's Fourth Amendment rules continue to treat different places in different ways.[108] Privacy has given us new protections in new contexts, but

---

[104] Olmstead v. United States, 277 U.S. 438, 465 (1928).

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

[106] Crocker, *supra* note 103, at 59.

[107] *Katz*, 389 U.S. at 351.

[108] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809 (2004) ("[T]he basic contours of modern Fourth Amendment doctrine are largely keyed to property law.").

property still remains.[109] Similarly, as we transition to a Fourth Amendment based on power not privacy, we should expect to continue to talk and think about privacy for many years.

Moreover, what property and privacy have in common is that they were both imperfect proxies for what the amendment actually protects. Until the advent of the telephone, property served as a bright-line proxy for the border between state scrutiny and private action. With the rise of the telephone, airplanes, and heat-sensing devices, privacy stood as an imperfect, but still reasonable, proxy for drawing that same borderline.

With the rise of widespread intermediation, portable sensing, and content storage, privacy is no longer serving as an appropriate proxy. The new constitutional lodestar, power, is the Fourth Amendment's third act. There is reason to believe, however, that this might be the final act. Power seems to be the amendment's essence, not merely a proxy for something deeper. If power (and liberty) is not the core of the amendment, it is close to being so, much closer than anything we have used before.

B. Private Power and State Action

In the coming world, when the police outsource surveillance to private third parties, a revised Fourth Amendment focused on maintaining a constitutional balance of power should cast much more scrutiny than it does today on how the private choices of private actors can disrupt this balance of power. But constitutional jurisprudence, built firmly atop a foundation of state action, does not lend itself easily to the idea that private action can give rise to constitutional problems.[110] This seemingly fundamental barrier to the development of a new foundation for the Fourth Amendment misses an important point. With the rise of the sur-

---

[109] Shortly before the final editing stages of this Article, the Supreme Court decided the landmark GPS-tracking case, *United States v. Jones*, 132 S. Ct. 945 (2012). The majority opinion by Justice Scalia embraces a decidedly property-centric view of the Fourth Amendment. *Id.* at 949.

[110] This is similar to, but ultimately different from, the welcome attention David Sklansky has paid to the private police. *See* Sklansky, *supra* note 41. Sklansky's discussion of the legal implications of the private police involves a rich account of the state action doctrine as it has been applied to criminal procedure, a topic that "has been largely neglected both by constitutional scholars and by criminal procedure scholars." *Id.* at 1230.

veillance society and the concomitant decline of police self-help, although the police will no longer be collecting information in the initial instance, they will still need to request the information from some third party, an unambiguous state action.

In the future, the police request alone will satisfy state action. This form of state action will seem different from the kind we witness today in two seemingly important ways that courts should acknowledge without getting too bogged down. First, the "action" of the state will seem thin compared to the cases we think about today. The police will not be climbing telephone poles or running packet sniffers, but instead will receive DVD-ROMs by messenger. Second, although tomorrow's state-action requirement will be met by little more than a simple police request, this should not bar a jurisprudence of Fourth Amendment "reasonableness" that focuses on the contents and structure of databases held by private parties, which means that the constitutionality of a search under the Fourth Amendment might depend on what happened during the time before state action. The decision of reasonableness might turn, for example, on why a private company has, say, a database tracking the location of private citizens to begin with, which will lead to a constitutional decision that will turn on pre-state-action facts.

C. Equilibrium Adjustment and the Surveillance State

How then does a Fourth Amendment designed to limit undue government power operate? What takes the place of the venerable reasonable expectation of privacy test, and do we preserve the historically important role of the warrant and probable cause requirements?

1. The Equilibrium-Adjustment Theory

In his recent article, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, Professor Orin Kerr identifies an underappreciated but, to his mind, near-universal goal driving how the courts have interpreted the Fourth Amendment in the face of technological change: balance[111] Kerr argues:

---

[111] Kerr, *supra* note 4.

> When changing technology or social practice makes evidence substantially harder for the government to obtain, the Supreme Court generally adopts lower Fourth Amendment protections for these new circumstances to help restore the status quo ante level of government power. On the other hand, when changing technology or social practice makes evidence substantially easier for the government to obtain, the Supreme Court often embraces higher protections to help restore the prior level of privacy protection. Fourth Amendment protection resembles the work of drivers trying to maintain constant speed over mountainous terrain. Judges add extra gas when facing an uphill climb and ease off the pedal on the downslopes.[112]

Kerr is adding rigor to several common intuitions about the Fourth Amendment: it should be technology-neutral and it should protect a level playing field.[113] Kerr argues that he has identified a theory that finds common ground among almost every Supreme Court Justice and interpretative theory that has ever tackled constitutional search and seizure. He argues that his "equilibrium-adjustment" theory can explain the approach of living constitutionalists, textualists, and originalists alike.[114]

Kerr is onto something. He identifies a pervasive and underappreciated thread running through the Fourth Amendment jurisprudence of technological change. I share his enthusiasm for this construct and his optimistic belief that we might be able to use it—properly fleshed out—to both rationalize some of the hard-to-theorize differences in doctrine as well as convince those who disagree about a given outcome that they are closer together than they appear.

Kerr's theory does a reasonably good job rationalizing past cases. For example, he convincingly explains how equilibrium adjustment can explain the "rather strange line" that regulates the use of tracking beepers by the police—no warrant needed on city streets but warrant needed inside the home[115]—as the Court's

---

[112] *Id.* at 480.

[113] *Id.*

[114] *Id.* at 526-27.

[115] *See* United States v. Karo, 468 U.S. 705, 714-15 (1984); United States v. Knotts, 460 U.S. 276, 282 (1983). Kerr wrote his article before the Supreme Court revisited

attempt to draw lines to try to maintain balance in the face of technological change.[116] He likewise does a nice job bringing a bit of coherence and rigor to the automobile cases, which hold that people enjoy fewer Fourth Amendment protections in cars than in other contexts, a notable accomplishment given how the judges themselves tend to provide only thin justifications.[117] Whereas these judges offer platitudes about how the mobility of automobiles can thwart crime fighting, or hopelessly circular arguments about how we expect less privacy in vehicles that are so often stopped without a warrant,[118] Kerr argues that the exception has stemmed mostly from equilibrium adjustment, and from attempts to level the playing field.[119]

But these two examples share one important feature in common—they each involve a technology that benefits only one side of the crime-fighting equation: the police (tracking beepers) or the criminals (automobiles). Kerr's theory, at least as he explicates it, performs not nearly as well when applied to new technologies used by "both criminals and the police."[120] Notably, most of the technologies in this problematic category tend to be the very same technologies that are the focus of this Article, technologies developed by private parties for private purposes that generate records useful to the police.

2. The Problem with the Balance Sheet Approach

When faced with technologies that create avenues for both committing and detecting crime, the problem for equilibrium adjustment is trying to figure out how to account for which direction and by how much the level playing field has shifted. The advent of the telephone made the life of a criminal both easier and more difficult. The theory of equilibrium adjustment requires us to determine which of these two impacts outweighs the other.

---

tracking beepers in *United States v. Jones*, 132 S. Ct. 945 (2012), decided shortly before this Article entered its final editing stage.

[116] Kerr, *supra* note 4, at 499-501.

[117] *Id.* at 502-08.

[118] *E.g.*, California v. Carney, 471 U.S. 386, 392 (1985) (explaining that automobiles deserve a "reduced expectation of privacy" because they are so often searched without a warrant).

[119] Kerr, *supra* note 4, at 507-08.

[120] *Id.* at 489.

Kerr tackles this problem using an informal accounting.[121] A judge should "recreat[e] the same limits on surveillance over the telephone network that exist on equivalent surveillance in the physical world."[122] The judge must account for all of the upsides and downsides the telephone brought to crime and crime fighting by comparing the new balance of the playing field to the one that existed before the invention of the phone.[123] To answer this empirical question, Kerr seems to suggest that judges should make lists that summarize the technological pros and cons experienced by criminals or the police.[124] This is not precise and feels intuitive and squishy. It turns out to be a messy, imprecise undertaking.

Perhaps too conveniently, Kerr's informal accounting leads him to support precisely the mix of Fourth Amendment rules we have today. Telephone surveillance, Kerr argues, triggers the Fourth Amendment because "the contents of phone calls . . . played the modern-day role of private meetings that were protected" before the telephone.[125] "As a result, the power to monitor communications in a phone booth when a person placed a call was the modern equivalent to the power to break into a home and listen to conversations there."[126] With this part of the analysis, I agree.

Where I disagree with Kerr is in his treatment of non-voice surveillance of numbers dialed. Pen registers and trap and trace devices should not trigger the Fourth Amendment under equilibrium adjustment he concludes, because they help level the playing field in favor of the police to make up for the advantages felt by criminals.[127] "The telephone network," Kerr explains, "provides criminals a substitute for traveling out in public and then meeting with conspirators in private, and the *Katz/Smith* line maintains the equilibrium of privacy that existed with the physical meeting for the telephone equivalent."[128] For this proposition, he does not cite studies or specific cases; this is an exercise mostly in common

---

[121] *Id.* at 512-17.
[122] *Id.* at 513.
[123] *Id.* at 512-17.
[124] *Id.*
[125] *Id.* at 515.
[126] *Id.*
[127] *Id.* at 516-17.
[128] *Id.* at 517.

sense intuition. Because the telephone has tilted the playing field too far in favor of criminals, Kerr concludes that, at least for pen register and trap and trace surveillance, the courts should create a rule weighted in favor of the police: the police should be allowed, without a warrant, to compile a list, in real time, of the circle of people a person communicates with on the phone in order to restore a power they used to have before the phone.[129]

Unfortunately, this informal accounting fills in only half of the balance sheet. The criminals are not the only ones who benefited from the rise of the telephone.[130] Telephone companies develop sophisticated systems of private surveillance that collect new pieces of information about communications (and, by simple extension, relationships and conduct) that once were never stored anywhere. Because these records—most importantly the record of calls made—get stored by default and retained for a long time, the police can recreate past behavior dating back before the target was even a target. The telephone, in other words, dramatically improves law enforcement's ability to conduct ex post investigations when compared to pre-telephone, physical world crimes. Crimes committed in the physical world, say stalking or the whispered conversations between co-conspirators, do not leave permanent records as a matter of course. In the pre-telephonic era, the police did not know where to look until the crime was detected and

---

[129] *Id.* ("Under *Smith*, the police can watch the network equivalent of public space to learn who the suspect called and when.").

[130] I am not the first to lodge this critique at Kerr. In response to an earlier, less-developed version of the argument, which Kerr called one of substitution effects, several commenters made similar points. *See, e.g.*, Erin Murphy, *The Case Against the Case For Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1244 (2009) ("[I]t seems probable that the more that third-parties are involved or technology is deployed, even with a robust conception of third-party protections, the more likely it becomes that the criminal will be apprehended. This is for the simple reason that enlisting third-party assistance in crime tends to generate, rather than obfuscate, opportunities to get caught. Third parties increase the possibility that a trail will be left or witnesses will be created, all of which only helps the state in building its case."); *see also* Blake Ellis Reid, Note, *Substitution Effects: A Problematic Justification for the Third-Party Doctrine of the Fourth Amendment*, 8 J. TELECOMM. & HIGH TECH. L. 613 (2010). "The neutrality argument, however, relies on the false premise that law enforcement has an *unlimited* capability to surveil low-tech public activities and a limited capability to surveil high-tech private activities. As discussed below—both generally and in the context of *Miller* and *Smith*—the opposite is often true." *Id.* at 620.

reported. The phone, in other words, has made crime fighting much easier.

This problem is not specific to telephones. Kerr's balance sheet approach is hard to use with any new technology for many reasons. First, every technology is a moving target, so it is a daunting task to ask a judge to characterize it accurately at one frozen moment in time. Second, lawyers and judges quite often explain and understand technology using analogies and metaphors. But, analogical comparisons seem to be a poor tool for a judge trying to make the kind of accurate and detailed accounting Kerr proposes.[131]

Third, most complex technologies present multiple levels of generality, and it is not clear at which level of generality the court should focus. For example, assume a court had to apply Kerr's test not to the 1970's *Smith v. Maryland* telephone network, but instead to the 2012 telephone network. Weighing both pros and cons, do criminals experience a net benefit or burden from the shape and configuration of the modern phone network? The court faced with this question will face a dizzying array of levels of generality. The traditional circuit-switched network discussed in *Smith* was made less private, and thus less useful for criminals, with the introduction of Caller ID.[132] Then again, Caller ID can be disabled easily in most places.[133] Similarly, the privacy of a telephone line has been altered through the introduction of technologies like Signaling System 7, which separates control signals from the content of voice conversations and creates something like a structural "envelope" around phone calls.[134] Then again, laws like the Communications Assistance for Law Enforcement Act obligates telephone companies to ensure the easy wiretapability of digital phone switches. And we have not even considered the

---

[131] Professor Kerr himself has written about the perils judges face applying analogues for new technology. *See* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357 (2003).

[132] Glenn Chatmas Smith, *We've Got Your Number! (Is It Constitutional to Give It Out?): Caller Identification Technology and the Right to Informational Privacy*, 37 UCLA L. REV. 145, 149-50 (1989).

[133] *See* FCC Calling Party Telephone Number Privacy Rule, 47 C.F.R. § 64.1601 (2005) (mandating per-call blocking of Caller ID for interstate calls).

[134] *See* Jonathan Jacob Nadler, *Give Peace a Chance: FCC-State Relations After California III*, 47 FED. COMM. L.J. 457, 502 n.229 (1995).

Internet yet.[135] If you include VoIP, Skype, and Google Voice, the already murky becomes almost entirely inscrutable.[136]

Fourth, as we work our way down the back-and-forth, pro-and-con list making of the kind just demonstrated, we are never told by Kerr when to stop. Consider once again the pros and cons of the telephone. Telephones make it harder to catch harassers, Kerr reasons, by letting them stalk their victims from the comfort and privacy of the home.[137] But, on the other hand, as discussed above, crimes committed in the real world do not routinely leave detailed records behind, so the life of the police has been made easier. Unless, of course, we analogize stored phone records to how eyewitnesses in the real world get to see suspicious people driving around town just before the crime. But, on the other hand, eyewitnesses may not be nearly as reliable as the stored record of an incriminating phone call. This is what happens with the balance sheet approach: each side of the ledger will grow and grow, and we will be locked in a state of seemingly infinite regress.

Fifth, and finally, assume we find our way out of infinite regress. What then? We will be left with two impressively long lists. New technology has both made it easier to commit and to fight crime. What does this mean for the Fourth Amendment? The easiest conclusion is Kerr's: to assume that the pros and cons cancel each other out, leaving us with a tool that does little more than justify the rules we have today.[138] That seems too coincidental to be useful. For these five reasons, the balance sheet approach is not redeemable. We need another, more objective, and more rigorous way to measure the effect of a new technology on crime and crime fighting.

3. New Metrics for Equilibrium Adjustment

The answer is to ask the question much more directly, never losing sight of our new normative goal, the preservation of the

---

[135] 47 U.S.C. §§ 1001-10 (2006).

[136] *See In re* Commc'ns Assistance for Law Enforcement Act and Broadband Access and Servs., 20 FCC Rcd. 14,989 (2005) (granting Justice Department petition to extend authority of CALEA to VoIP services).

[137] Kerr, *supra* note 3, at 578.

[138] Kerr, *supra* note 4, at 517 ("Taken together, *Katz* and *Smith* maintain the balance of power over the shift from physical surveillance to telephone surveillance.").

balance of power between the citizens and the police. The ultimate question should be: How has technology altered the *metrics* of crime fighting? Are more people going to prison? Fewer? Are leads easier to develop today? Harder? How long does each investigative step take to accomplish? Here is an admittedly unorthodox proposal: it should take, on average, just as long to solve a crime today as it has in the past. Through the Fourth Amendment the Framers provided a fixed ratio between police efficiency and individual liberty, and as technological advances change this ratio, judges can interpret the amendment in ways to change it back.

Some might react negatively to the idea that the Constitution mandates an inefficient constabulary, particularly in cases of ongoing victimization.[139] But throughout the history of Fourth Amendment jurisprudence the courts have enacted rules and holdings that force the police to be more inefficient in their duties than they would be without these rules and holdings. Every procedure imposed by the Fourth Amendment (and the Fifth and the Sixth, too) creates a more inefficient constabulary. Warrants take time to draft; subpoenas get met by motions to quash; and probable cause develops slowly. Until now, police efficiency standing alone has not amounted to unconstitutionality. If we reconceive of the Fourth Amendment as a regulator of power and liberty, not merely privacy, it is hard to see why the Constitution would prohibit such a construction.

A Fourth Amendment that forces police inefficiency might also be defended simply as a mirror image of the current Fourth Amendment, which often generates new rules designed to ensure criminal inefficiency. When criminals find a new tool of efficiency, such as the automobile, the Court will often decrease Fourth Amendment protections in order to rebalance the privacy/security balance that is supposedly at the heart of the reasonable expecta-

---

[139] In fact, the Supreme Court has said as much, albeit speaking decades before the rise of the surveillance state. In *United States v. Knotts*, which involved the use by police of tracking beepers, responding to defendant's argument that tracking beepers made the police too efficient, the Court rejoined, "Insofar as respondent's complaint appears to be simply that scientific devices such as the beeper enabled the police to be more effective in detecting crime, it simply has no constitutional foundation. We have never equated police efficiency with unconstitutionality, and we decline to do so now." 460 U.S. 276, 284 (1983).

tion of privacy test.[140] Under current Fourth Amendment jurisprudence, insecurity justifies creating artificial criminal inefficiency; under the new Fourth Amendment jurisprudence, excessive government power will justify creating artificial police inefficiency.

Once we shift our view from privacy to power, we can better articulate the need for mandated police inefficiency. General warrants were powerful tools of efficiency, yet they went too far toward permitting arbitrary exercises of power on the colonies and tread too much on the liberties of the colonists. Today, with new technology, the police can often come close to exerting the power of the general warrant, as I have argued in a slightly different context.[141] A new Fourth Amendment attuned to problems of government power might need to resort to mandated police inefficiency in response.

D. Beyond Warrants and Probable Cause

Equilibrium adjustment can help judges determine whether to turn the Fourth Amendment's tuning knobs to restore the level playing field. But it will not do enough to safeguard liberty from undue governmental power unless we also add a few new tuning knobs.

A new Fourth Amendment designed to enforce the level playing field must address the misconception that the warrant and probable cause requirements represent the high water mark, the most onerous and liberty-protective things that may be imposed on the government. The very development that brought us to this point, the rise of the surveillance society, instead reveals that the warrant and probable cause requirements are often quite toothless requirements that the government will be able to meet with ease. It is a good thing that in their wisdom (or with luck), the Framers did not bind the Fourth Amendment solely to warrant

---

[140] Carroll v. United States, 267 U.S. 132, 151 (1925).

[141] Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1, 11 (2011), http://www.virginialawreview.org/inbrief/2011/03/20/ohm.pdf ("Computer search warrants are the closest things to general warrants we have confronted in the history of the Republic.").

and probable cause but instead required the much more flexible requirement of reasonableness.[142]

In earlier work, I have argued that too much attention has been paid to the probable cause requirement.[143] Especially in debates over the proper Fourth Amendment requirements for access to electronically stored information like e-mail, the only requirement that gets serious attention is whether or not the police must show probable cause before access is allowed.

But I have argued that investigations that take place on networks differ from those in the physical world in five ways that all conspire to give the police probable cause in most circumstances:

> First, evidence online almost always comes surrounded by a rich context, providing a high level of built-in suspicion to a suspicious e-mail or IP address. Second, the path from victim back to suspect is fixed and often traceable. Third, the "eye witnesses" online tend to be sophisticated corporate intermediaries without relevant biases or agendas. Fourth, these intermediaries and the victims themselves deploy pervasive systems of surveillance. Fifth, these surveillance systems record precise, unambiguous evidence.[144]

All five of these features apply to the systems of private surveillance discussed in Part I. As the police shift from self-help to outsourced surveillance, and as they morph from producer to consumer of surveillance data, they will often find themselves awash in probable cause. Increasingly, it will seem odd to us that probable cause once seemed like an onerous burden. As the probable cause and warrant requirements cease playing a meaningfully disciplining role in many contexts, courts should find within the Fourth Amendment's requirement of "reasonableness" many additional requirements.

For ideas on what other types of restrictions on the police reasonableness might require, courts should look to Congress. One good source for such restrictions is the Electronic Communications

---

[142] Amar, *supra* note 74, at 762-85 (arguing against the pervasive idea that the Fourth Amendment requires warrants and probable cause).

[143] *See* Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514 (2010).

[144] *Id.* at 1529.

Privacy Act (ECPA).[145] In this law, Congress has found many other parameters to control aside from the mere suspicion standard. Some parts of this law require notice to the person whose records are being requested[146] and others do not.[147] Some require judicial review,[148] while others require only internal approval.[149] Among the parts of this law that require judicial review, some require searching review,[150] while others are much more minimalist.[151] Some surveillance can be conducted only in certain types of criminal investigations.[152]

In addition to all of these, the courts should consider availing themselves of a tuning knob that they have too rarely deployed, the necessity requirement, as I have argued elsewhere.[153] The necessity rule is a rule about timing. The rule provides that the court has deemed that a given police procedure is so invasive that the police must refrain from using it until late (or last) in their investigation.

Congress, again, has modeled the need for and efficiency of the necessity requirement in the federal wiretap act. Section 2518(c), Title 18 of the United States Code requires that the application for warrant include "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous."[154]

If a particular type of private surveillance tilts the balance of power in favor of the police too far, the court can find within the Fourth Amendment's requirements a new necessity rule: when the

---

[145] ECPA was first enacted in 1986 as the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986), and has been amended many times since. *E.g.,* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. 107-56, §§ 209(2), 210, 212(b)(1), 220(a)(1), 220(b), 115 Stat. 283, 285, 291, 292 (2001). The Act amended and added scattered provisions throughout Title 18.

[146] 18 U.S.C. § 2703(b)(1)(A) (2006).

[147] *Id.* § 2703(b)(1)(B).

[148] *Id.* § 2518.

[149] *Id.* § 2703(b)(1)(B) (permitting access to certain records with a mere subpoena).

[150] *Id.* § 2518(3).

[151] *Id.* § 3123(a)(1).

[152] *Id.* § 2516.

[153] Ohm, *supra* note 143.

[154] 18 U.S.C. § 2518(c) (2006).

police seek to monitor the records created by the third-party provider in the particular context (say location information), it should be required to first show that "other investigative procedures have been tried and failed . . . [or are] unlikely to succeed if tried or to be too dangerous."[155] Just because my smartphone tracks my location, this does not give the police the right to follow me around town when they could tail my car or install a tracking beeper instead.

Until the courts get around to implementing this kind of rule, Congress should consider doing it. A good candidate is cell phone location tracking. At the time this Article was written, at least four bills had been introduced in the then-current Congress, which focused on the emerging problem of cell phone tracking.[156] At least two of these would have imposed a probable cause warrant requirement on the police before they could obtain prospective records of cell phone tracking.[157] In addition, Congress should consider requiring proof of necessity. Cell phone tracking, just like wiretapping, should not be allowed until "other investigative procedures have been tried and failed."[158]

The courts should learn an important lesson from the many tuning knobs of ECPA: there are many ways to rebalance the playing field of criminal investigation beyond the warrant and probable cause requirements, and the Fourth Amendment can incorporate them. The courts should feel free to superintend police procedures in new, creative ways, following Congress's lead. This is true no matter which way the playing field has tipped, either in favor of the police or the criminals. Let us consider each case in turn.

In situations when the metrics suggest that a new tool has tilted the playing field to criminals too much, making investigations much longer or increasing the number of unsolved crimes, rather than rolling back all Fourth Amendment protections, the Courts should consider stepping to a middle ground by requiring

---

[155] *Id.*

[156] Location Privacy Protection Act of 2011, S.1223, 112th Cong. (2011); Geolocation Privacy and Surveillance ("GPS") Act, S.1212, 112th Cong. (2011); Electronic Communications Privacy Act Amendments Act of 2011, S.1011, 112th Cong. (2011); Commercial Privacy Bill of Rights Act, S.799, 112th Cong. (2011).

[157] S.1212 § 2; S.1011 § 5.

[158] 18 U.S.C. § 2518(c) (2006).

the kind of sub-warrant judicial approval embodied in ECPA's "d-order" standard.

According to 18 U.S.C. § 2703(d), some types of surveillance are permitted only when the government "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."[159] Many have compared this to the standard of *Terry v. Ohio*, the stop-and-frisk standard that allows limited police inspection with less than probable cause.[160]

On the other hand, when a warrant requirement backed by the probable cause standard is found not to be enough, and a new technology made available by private providers shifts the playing field too far toward the government, making the police so hyper-efficient that it offends the balance of power promised by the Fourth Amendment, courts should feel free to require additional burdens on the police, such as new necessity requirements.

E. Putting the Pieces Together

1. The Default Rule

We are left with the problem of the default rule. When we are faced with very new technological advances, and before we know whether these advances have aided law enforcement or criminals more, should the rules impose significant burdens on the police, zero burdens on the police, or something in between? One way we can choose is to ask who should bear the cost of errors.

Today's default rule, in the form of the third-party doctrine, places the cost of errors on society not the police. In most emerging situations, the police can access the fruits of private surveillance without a warrant or probable cause.

The opposite result is the better one. The cost of errors should be borne first by the police. Whenever a private company enables a new form of surveillance, the police should be forced to assume

---

[159] *Id.* § 2703(d).

[160] United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008); ORIN S. KERR, COMPUTER CRIME LAW 515-16 (2006); U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 131 (3d ed. 2009), *available at* http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf.

that access to the fruits of the surveillance require a warrant and probable cause until we know (with the assistance of metrics) that the new service benefits criminals more than it helps the police.

A textual analysis of the amendment supports this conclusion. The amendment prohibits unreasonable searches and seizures. It does not guarantee for police the minimal burdens possible. The right is for the investigated not the investigator.[161] If Congress passes a law permitting the search of a home without a warrant, the law is unconstitutional and void. On the other hand, if Congress passes a law forcing the use of a warrant in situations where the amendment would require none, this is fine, because it is well within the prerogative of legislatures to require more protection than the Constitution provides.

There is one last reason to favor this default rule. The metrics at issue will largely be controlled by the police. Creating a default rule of no process needed gives the police the incentive to drag their feet or obfuscate statistics. On the other hand, placing the benefit of delay against the party likeliest to delay will help improve the overall legitimacy and efficiency of the process.

2. Breaking the Link Between the Surveillance Society and State

Putting the pieces together, when a court must resolve a Fourth Amendment challenge to police access to information stored by a third party, particularly in cases involving new technologies like networked communications, the police must present statistics quantifying the effect the technology in question has had on criminal investigations. Having thus introduced the basic idea, this Article will not also proceed to try to identify the very best set of statistics to measure, which it expects to be the subject of much debate and litigation, should this approach ever be embraced.

If statistics are unavailable or hard to interpret because the technology is new, then the police may access the information only with a warrant and probable cause, because of the default rule. If

---

[161] Similarly, Morgan Cloud, considering the "two conflicting value-based assumptions" of the Fourth Amendment, one which "favors efficient law enforcement, the other favors individual liberty," chose liberty "as the *grundnorm* of the amendment" based on the "history and text of the amendment." Cloud, *supra* note 93, at 296.

the statistics indicate that the technology has greatly hampered law enforcement, by letting criminals evade detection by hiding once-visible activity online, then the court will decrease the requirements of the Fourth Amendment for access to the data, perhaps to a mere subpoena or by relaxing the requirement of notice to the user. Finally, if statistics indicate that even with a warrant and a probable cause, the technology has shifted the playing field too far to the benefit of the police, the court can impose new burdens on the police such as a requirement of necessity.

CONCLUSION

For nearly fifty years, privacy has served as a useful proxy for deciding what the Fourth Amendment protects. As we witness the rapid decline of privacy, we should be prepared to rebuild the Fourth Amendment on a new foundation focused on the balance of power between the state and its citizens.

The shift from privacy will be a disruptive one, and we will be forced to abandon long-held intuitions and maxims. One especially important one that deserves some attention before we let it go is the centuries-old maxim that police on the street need not "avert their eyes" from crime in public.

The maxim is ancient and was already established by the time Lord Chief Justice Camden wrote in *Entick v. Carrington* that "the eye cannot by the laws of England be guilty of trespass."[162] It is hard to argue with the logic behind it. There is a deeply intuitive appeal to the idea that we cannot ask police officers, sworn to protect and thrust in harm's way, to ignore what is

---

[162] 19 How. St. Tr. 1029 (1765), 95 Eng. Rep. 807 (K.B. 1765). The full quote lends support for the argument that the police need limits with respect to private papers:

> Papers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect. Where is the written law that gives any magistrate such a power? I can safely answer, there is none; and therefore it is too much for us without such authority to pronounce a practice legal, which would be subversive of all the comforts of society.

19 How. St. Tr. 1029 (1765).

right in front of them. It is hard to believe that the Framers would have intended such a result. Forcing the police to shift their eyes in physical, public places seems an unwise shift in the constitutional balance between privacy and security.

But once you move from a Fourth Amendment built on privacy to one built on power, the unassailable logic breaks down. We certainly have never presupposed that the police are entitled to every fact about behavior on earth. The list of the things the police officer on the sidewalk is prevented from learning about the activity in the immediate vicinity is much, much longer than the list of facts he can observe, because he is subject to two types of constraints, one set by the laws of physics, the other by the laws of man. On the sidewalk, the laws of physics predominate. Things happening behind walls and closed doors are unseen; conversations whispered a block away or coursing through the wires overhead are unheard; and heat patterns emanating through walls are undetected. The world—the physical world—is rich with natural, physical constraints like these.

Technology can war with physics, giving the police the ability to enhance their senses, making natural constraints irrelevant. With a wiretap, the police can listen to the conversations on the wires, and with a thermal imager, the police can detect invisible heat patterns. But in both of these cases, the Supreme Court has decided that these tools upset the constitutional balance toward security and away from privacy too much, and it has replaced the vanished physical constraint with a legal constraint.[163]

Consistent with these cases, we should view the police officer on the sidewalk as a complicated story of constraints, some imposed by physics and some by law. I am arguing that today, many structural constraints are falling away.[164] Until the recent past, business practices (and the laws of physics) provided many well-tailored "structural rights in privacy."[165] Private companies, by

---

[163] Kyllo v. United States, 533 U.S. 27, 40 (2001); Katz v. United States, 389 U.S. 347, 358-59 (1967).

[164] *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009); Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605 (2007).

[165] Surden, *supra* note 164, at 1617-18.

convincing us all to carry tracking beepers and to post status updates, have knocked down these structural rights in privacy.

Now that we are losing structural constraints of privacy, sometimes the Fourth Amendment might force the police to avert their eyes to easily and readily obtainable facts, just as it has done in other contexts.[166] But where wiretapping and thermal imaging used to seem the exception not the rule, soon, our default stance should be to deny the police easy access to newly revealed facts out in the world. This is not unnatural, nor embarrassing, nor regrettable. It is the direct consequence of the new Fourth Amendment, which polices power not privacy, and one which serves as an important bulwark of liberty in these changing times.

---

[166] *Cf.* David A. Sklansky, *Back to the Future:* Kyllo*,* Katz*, and Common Law*, 72 MISS. L.J. 143, 210 (2002) ("In the long term, sensible interpretation of the Fourth Amendment will require the Court to acknowledge the differences between government surveillance and private snooping, and to abandon the assumption that anything knowingly exposed 'to the public' is therefore fair game for the police.").