# The Cambridge Handbook of Surveillance Law

Edited by
**David Gray**
University of Maryland

**Stephen E. Henderson**
University of Oklahoma

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

One Liberty Plaza, 20th Flo , New York, NY 10006, USA

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pu suit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107137943
DOI: 10.1017/9781316481127



First published 2017

Printed in the United States of America by Sheridan Books, Inc.

*A catalog record for this publication is available from the British Library.*

*Library of Congress Cataloging-in-Publication Data*
Names: Gray, David, editor. | Henderson, Stephen E., editor.
Title: The Cambridge handbook of surveillance law / edited by David Gray, University of Maryland; Stephen E. Henderson, University of Oklahoma.
Description: New York: Cambridge University Press, 2017. |
Includes bibliographical references and index.
Identifiers: LCCN 2017009648 | ISBN 9781107137943 (hardback)
Subjects: LCSH: Electronic surveillance – Law and legislation – United States. | Intelligence service – Law and legislation – United States. | Terrorism – Prevention – Law and legislation – United States. | National security – Law and legislation – United States. | Computer security – Law and legislation – United States. | Computer networks – Security measures – United States. | Cyberterrorism – Prevention – United States. | United States. Privacy and Civil Liberties Oversight Board. | Privacy, Right of – Government policy – United States.
Classification: LCC KF5399.C36 2017 | DDC 345.73/052–dc23
LC record available at https://lccn.loc.gov/2017009648

ISBN 978-1-107-13794-3 Hardback

# 17 An Eerie Feeling of Déjà Vu: From Soviet Snitches to Angry Birds

Judge Alex Kozinski[†] & Mihailis E. Diamantis[‡]

The U.S. government knows a lot about us. Literally, from the moment we're born to the moment we die, it tags and monitors us. We provide some of that information on the forms we file for licenses, taxes, and major life events. Much of the rest the government collects, without our help, using security cameras, body scanners, license plate readers, and the like. But the data the government gathers itself is a small drop in the ocean of information we constantly generate.[1] Every time we open a bank account, use a credit card, email a friend, upload a video, browse the Internet, make a phone call, create and store a digital file, or go anywhere with a cell phone in our pocket, we shed reams of very personal information. Even while sleeping, most of us generate data that someone's interested in, if only as evidence of inactivity.

To collect and analyze this sort of information, governments need to outsource to private parties. The traditional way to do this, and the old favorite of totalitarian regimes like the Soviet Union, is to recruit the citizenry. Get them to spy on each other and report back. That method is clumsy, but effective to an extent. The slicker, modern approach used in the United States (and almost everywhere else now) relies on the private sector – the corporations that collect our data in the ordinary course of business. This includes just about every corporation that interacts with individual customers, and many more besides, from banks, cell phone companies, and Internet service providers, to loan collectors and straight-up data collectors watching on the sidelines. These corporations meticulously record every transaction we have with them, and many transactions we don't. For a price, it's all transferable to the government – or anyone else willing to pay – with the click of a button: no need for dark alleys and hushed voices.

These two approaches raise overlapping concerns. We expose our most vulnerable and intimate details to the private parties we love and trust, the neighbors and corporations we interact with on a daily basis. Through these private interactions, we develop those idiosyncratic personal identities that are the lifeblood of American individualism,

[†] Judge, United States Court of Appeals for the Ninth Circuit.
[‡] Associate Professor, University of Iowa, College of Law.

[1] Some put this number currently at three to ten data points per second. Theresa M. Payton & Theodore Claypoole, Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family 12 (2014). Everyone expects that number to mushroom in the coming years.

the engines of our innovation, and the seeds of our social progress.[2] The privacy of that space is crucial; if the secrets revealed in it are openly available to those with the power to punish us, it disappears. Censorship, even if self-imposed, is the enemy of the free.

How can we protect this private space in America today? We live in a world where we generate and record literally two and a half quintillion bytes of data every day.[3] We have no choice but to trust almost all of this data to the private third parties who transmit and store it. And these third parties have strong financial and legal incentives to turn much of it over to the government. This is not the first time a society has had to deal with omnipresent private informants. The experiences of regimes like the Soviet Union hold lessons for the rise of private surveillance today.

## I Soviet Snitches

Policing is largely about negotiating information asymmetries. The targets and the people around them are always going to know more about themselves, whether before they're suspected of anything, while they're being investigated, or during any trial. The asymmetry becomes more of an obstacle as a government tries to police more people and wider swaths of their lives. It could seem downright insurmountable to a totalitarian regime like the Soviet Union.

To cope, the Soviets recruited an army of private informants – and how! The number of private informants working for them peaked at around 20 million during World War II.[4] With a population of just less than 200 million, that means one in ten Soviets was in the business of ratting out his neighbors. Soviet-influenced East Germany trailed slightly, with one informant for every sixty-six citizens.[5] But with surveillance files on nearly a quarter of the population, East German officials were still very thorough.[6] The information these citizens relayed was crucial to the success of the Soviet and East German secret services.[7] Still, from a vantage where a 16-gigabyte thumb drive capable of holding nearly 11 million pages of text sells for less than ten dollars, it's hard to imagine just how much pencil sharpening this required. No one accused the Soviets of being halfhearted.

True to its egalitarian roots, the Soviet Union recruited informants in all social strata, from peasants to soldiers to clergy. That, after all, was the best way to get information *on* all social strata. Informants were divided into *osvedomiteli*, ordinary people who reported information in the course of their regular lives, and the *rezidenty*, to whom they reported. For the information network to penetrate into the most secret nooks of people's lives, instinctive protectionism toward friends and family had to be overcome. If their legends are to be believed, the Soviets succeeded. The best-known story told of a thirteen-year-old peasant named Pavel Morozov, who caught whiff that his father was secretly assisting

2 Sygmunt Bauman & David Lyon, Liquid Surveillance 28 (2013) ("Privacy is the realm that is meant to be one's own domain, the territory of one's undivided sovereignty, inside which one has the comprehensive and indivisible power to decide 'what and who I am' ").

3 Matthew Wall, *Big Data: Are You Ready for Blast-Off?*, BBC News (Mar. 4, 2014), http://www.bbc.com/news/business-26383058.

4 Robert W. Stephan, Stalin's Secret War: Soviet Counter-Intelligence Against the Nazis 61 (2003).

5 John O. Koehler, Stasi: The Untold Story of the East German Police (1999).

6 Gary Bruce, The Firm: The Inside Story of the Stasi 11 (2010).

7 James Heinzen, *Informers and the State under Late Stalinism: Informant Networks and Crimes against "Socialist Property," 1940–53*, 8 Kritika: Explorations in Russian & Eurasian Hist 789, 790 (2007).

other peasants outside the normal Soviet channels. As a true Soviet, Pavel dutifully reported this to authorities, and his father was executed soon after.

How do you get people to snitch, even on their most intimate associates? Instilling a sense of patriotic duty helps. Pavel's family didn't much appreciate his patriotism and killed him shortly after his father's trial. But Pavel's spirit would live on in a martyr's tale commemorated in hundreds of children's books. Still, as the family's response suggests, patriotism can only go so far. A bit of government-led blackmail can help drum up enthusiastic informants and was a common recruitment tactic. Once officials received reports against one person, they could offer lenience for reports on others in an ever-widening information Ponzi scheme. The Soviets didn't get all of their information from true patriots or through coercion. Just to be sure they covered all their bases, they also offered cold, hard cash in return for good information. As discussed further below, this mix of voluntary and involuntary informants is an important parallel to the way private surveillance works today.

What was the effect of this surveillance in the Soviet Union? In the United States, we might say something measured like "Awareness that the Government may be watching chills associational and expressive freedoms."[8] But this doesn't even begin to describe the dangers. Lavrenti Beria, the head of Stalin's secret police, famously proclaimed, "Show me the man, and I'll show you the crime." With that kind of power, you can wrap freedom in a bag and deep-freeze it.

## II Angry Birds

The U.S. government must also cope with information asymmetries between enforcement authorities and their targets. The events of September 11, 2001, prompted a frenzied effort to close the information gap. In this, the U.S. government had an advantage the Soviets did not: modern commerce, and its extremely sophisticated, ready-made information-gathering infrastructure. Long before 2001, private corporations logged just about everything they could find out about us. Every step we took, whether we liked it or not, was recorded, sorted, packaged, and sold to advertisers. The government just had to sign up as one more customer of the data brokers. And with each passing year, the sort of information these corporations can get their hands on becomes more detailed and more personal. Eat your heart out, Lavrenti Beria.

Here's a typical business model for accessing customer data: Angry Birds is a great game. And better yet, it's free. How can Rovio, the developer of Angry Birds, be worth more than $1 billion if it gives away free software? It turns out it's much more profitable to watch you playing a free app than to try to sell it to you. And Angry Birds does watch you. Want to install the cool new take on the game, Angry Birds Transformers? At the time of writing, you must give the app and its developers access to your identity, the files and photos on your phone, control over your camera, and information about your calls and Wi-Fi connections. Earlier versions of the game, like so many other free apps, tracked your location, even while you weren't playing. All of this data allows Angry Birds to feed you tailored advertising that marketers will pay a high premium to secure. That's how Rovio pays its pricey coders to give us a streamlined experience without touching our wallets, while still turning an enviable profit.

8 *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

It's not only apps that do this. Almost anything you do that puts you in touch with a service provider produces a stream of information that is advertising gold. Some points of contact are obvious, as when we memorialize our personal data on social network sites like Facebook. In these cases, what may not be obvious is just how *much* of that data is collected and stored. When Austrian law student Max Schrems used European Union laws to force Facebook to give him a copy of the data they had on him, they sent him a 1,200-page PDF.

Other points of contact are less apparent, at least to the uninitiated. There are more than one hundred different companies that track just about every move you make on the Internet. You may never have heard of any of them, but they know you very well. They track you without disturbing your surfing experience and without even telling you. They do this by installing bits of data called "cookies" behind the scenes onto your computers. These cookies identify you and store information about your browsing history. On the basis of your Internet trail, when you visit a Web page, the advertising space is auctioned in real time to, for example, a pharma company that manufactures sleep aids; you might see their ad if the cookies on your system indicate you recently searched Wikipedia for information about insomnia. Some of this tracking data publicly purports to keep your identity hidden; others, such as code used by most popular sites, can track you directly back to your social networking profiles.

Your phone, and not just the apps on it, is like your personal homing beacon. Mobile phone carrier networks log your GPS data, tracking you throughout your day within a few meter radius. Even if you turn off GPS location tracking, cell companies can and do track you through the cell phone towers your phone automatically connects to. And even if you have no cell connection, companies track you using your phone's Wi-Fi and Bluetooth signals by planting devices on streets and in stores specifically for that purpose. Carrier networks sell the location data they gather to companies such as Sense Networks, which crunch it to create very specific user profiles. Advertisers then buy these profiles for targeted marketing.

Scrapping your cell phone and computer won't let you cut a hole in the corporate dragnet. Anytime you use a credit card, store membership card, bank account, etc., you produce data that private corporations collect and monetize. Even just driving your car, there's a good chance your location is being logged by any number of companies that mount license plate scanners on vehicles in their fleet. These companies got started with a mind to help lenders track down cars with defaulted loans, but now they track any car that comes within range. In the near-future, face scanners will supplement plate scanners and will biometrically log drivers, passengers, and pedestrians.

This frighteningly precise information is just the tip of the iceberg of customer data private corporations can, do, and will gather. But it's more than enough to show why Google CEO Eric Schmidt could, with a straight face, say, "We know where you are. We know where you've been. We can more or less know what you're thinking about."[9] Acxiom, one of the largest big data brokers, claims to have fifteen hundred data points on each of more than 700 million people. Those data points give them enough insight into your psychological makeup to fit you into hundreds of refined consumer categories, estimating, for example, how likely you are to pay cash for a new Korean vehicle.

[9] Derek Thompson, *Google's CEO: 'The Laws Are Written by Lobbyists'*, Atlantic (Oct. 1, 2010), http://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908.

It's private corporations collecting all this data. What's that got to do with the U.S. government? A lot, it turns out. Just as Soviet citizens could secure financial and political benefits by informing on their neighbors, it can be very profitable for American companies to sell customer data to the government. By one estimate, intelligence contracts with the U.S. government are worth $56 billion a year. With this kind of money on the table, it's unsurprising that the likes of Acxiom have worked hard to cultivate relationships with law enforcement. License plate scanners and cell companies, too, regularly send their information to police. And, yes, even Angry Birds has drawn the attention of U.S. intelligence organizations as a potential source of information.[10]

Dollar amounts aren't always publicly available, but those that are show just how lucrative sales to the government can be. AT&T, for example, charges the government twenty-five dollars per day to track a phone, and Sprint charges thirty dollars. At this price, the data sells for much more than the cell service of the customers they're tracking. But it's still a good deal for police, who send cell companies millions of data requests each year. The number of requests is so overwhelming that some cell service providers have set up automated Web interfaces for processing requests.

What the U.S. government can't get from private corporations with a financial carrot, it gets from them with an enforcement stick. They don't use Soviet-style blackmail tactics, but they have just as effective tricks available to them. As discussed in more detail later, the stick is backed up by a broad subpoena power federal officials can use to force corporations' hands. When the government exercises that power, it means business. In one instance, the National Security Agency threatened Yahoo with fines of $250,000 per day if it refused to turn over user data; that figure was set to double every week.

Despite some high-profile clashes between the government and private data brokers – like the one with Yahoo and the more recent one between the Department of Justice and Apple over encrypted user data on iPhones – the relationship between the two is generally cozy. As one leading commentator observes, "Corporate and government surveillance interests have converged."[11] Before Edward Snowden showed the public just how much information the government was collecting, tech companies by and large provided customer data to the government on request.[12] Now, in a bid to win back customer confidence, companies sometimes put up at least a pretense of resistance.

Today, as much as ever, private data broker and government interests are aligned along many dimensions. Commercially: Data brokers make good money when the government buys data that would cost much more to acquire itself. Logistically: Data corporations and the government rely on each other for amassing as much data as possible. Corporations have no choice but to get some of that information from the government, such as voter registration records or driver's license information. Government agencies have no choice but to buy this data back from the corporations once it's analyzed and supplemented with corporate databases. Professionally: Even if we don't know details, we do know there are secret meetings between top tech company CEOs and government intelligence agencies. These sorts of personal connections help build the well-documented

[10] Jordan Robertson, *Leaked Docs: NSA Uses 'Candy Crush,' 'Angry Birds' To Spy*, SF Gate (Jan. 29, 2014), http://www.sfgate.com/technology/article/Leaked-docs-NSA-uses-Candy-Crush-Angry-5186801.php.

[11] Bruce Schneier, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World 25 (2015).

[12] Robert Scheer, They Know Everything About You 19 (2015).

revolving door between the private and public intelligence professions, as personnel move freely between the two.

## III Consent, a Vanishing Privilege

One obvious difference between a Soviet neighbor fingering you to the government and Angry Birds doing the same is consent. The Soviet neighbor will peep in your window regardless. Angry Birds gains access to your information only after you click "I Agree." But this formalistic consent ritual amounts to true consent only for a wealthy and sophisticated few. The vast majority of users either don't know what they're "consenting" to, or don't really have a choice. Even for the rich and knowledgeable, withholding consent isn't always an option.

What do you "agree" to when you allow Angry Birds access to your location data and all your photos and files? Chances are high you don't have a clue. This is intentional. The privacy terms you formally agree to are usually available through some hyperlink, but you've got at least a couple of hurdles preventing you from reading them. These documents are long, sometimes dozens of pages, and seem longer still when reading them on a four-inch screen. Even if you're a fast reader, the value of the time it would take to go through the document line by line probably exceeds the value of the app. This even assumes you're capable of understanding what you read. The privacy agreements are written by lawyers and techies, for lawyers and techies, usually with no effort to make them penetrable to the vast majority of users. When the implications of such agreements are made apparent, as when the press let users know that Angry Birds was tracking their location and selling the data, users are shocked.

Suppose you are a lawyer with the extraordinary patience to read a privacy agreement. You may understand what you've agreed to formally. But unless you know a good deal about big data science, you probably have no idea what you've *really* agreed to. The app developers, and whomever else they sell your data to, will know the information you've allowed them to collect, but also everything they can infer from aggregating all that information. Those inferences are the most valuable part.

Suppose you agree to let Angry Birds collect anonymous location data. You may think you'll just appear in some database as a random number with a series of times and coordinates. False. There is no such thing as "anonymous" location data; this data *identifies you*. At MIT, researchers were able to identify by name 95 percent of Americans in a database from just four date/location points. Even if you agree to something much less voyeuristic than location tracking, such as providing your zip code, date of birth, and gender (some of the most common lines to register for any Web site), there's an 87 percent chance this data picks you out uniquely. The margin of error closes dramatically once brokers aggregate this data with that from other sources, and can triangulate among them all. Aggregation of different databases also exponentially increases the inferences data brokers can draw. Even if data brokers only have metadata, they can infer everything else if they aggregate enough of it. As former NSA general counsel Stewart Baker put it, "Metadata absolutely tells you everything about somebody's life. [With] enough metadata you don't really need the content."[13] Data brokers with Angry Birds' location data

[13] Alan Rusbridger, *The Snowden Leaks and the Public*, N.Y. Rev. of Books (Nov. 21, 2013), http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public.

can do much the same thing. If they can put you and a colleague in the vicinity of an out-of-town motel a couple of times, they probably know about your tryst. Did you agree to let them know *that*?

If you are sophisticated enough to understand – *really* understand – a privacy policy and its implications, you may have some options. Free apps that recoup their expenses by collecting and selling your data sometimes have paid versions that are less invasive. Other developers may make for-pay equivalents. Moving beyond apps, you can also register for subscription-based privacy-protective email services (such as Riseup) and cloud storage (such as SpiderOak) and software that masks your location and identity when you surf the Web. The cost of everything you'll need can add up. Julie Angwin, a former *Wall Street Journal* reporter, documented her various efforts to minimize the data private corporations could collect about her.[14] It wasn't cheap. And she had a persistent sense that rather than disappearing, she was raising red flags as a tin-foil-wrapped conspiracy nut.

Because of these costs, only a resourceful few actually have some option besides clicking "I Agree." Judge Kozinski may be prepared to pay up to twenty-four hundred dollars a year to protect his privacy, but, as he well knows, not everyone is so fortunate.[15] "Poor people are entitled to privacy, even if they can't afford all the gadgets of the wealthy for ensuring it."[16] This issue came to a head a few years ago over government use of tracking technology. In 2012, the Supreme Court decided that the government can't put a GPS device on your car without getting a warrant first.[17] But in the lead-up to that decision, the law, at least in the Ninth Circuit, was developing in a way that would have placed the poor – and even many middle class – at a distinct disadvantage. In *United States v. Pineda-Moreno*,[18] a Ninth Circuit panel concluded that a person has no reasonable expectation of privacy if he or she parks in an open driveway. Accordingly, without a fence and a gate, the government can attach GPS devices to a car anytime, warrant be damned. As Judge Kozinski pointed out in dissent, that's exactly the way you might expect federal appellate judges who live in gated communities and make more than $200,000 a year to think about the problem. But "the Constitution doesn't prefer the rich over the poor,"[19] and it should protect you equally, whether or not you can afford gates and guards and walls.

The worse off you are, the more invasive corporate surveillance becomes and the fewer options you have to prevent it. Consider single mothers on welfare. The state already has them picked out as surveillance targets to monitor the appropriateness of continued welfare support. For them, the state recruits all available resources, private and otherwise, in a panoptic machine what would make even seasoned criminals cower. "In their pursuit of food, healthcare, and shelter for their families, they are watched, analyzed, assessed, monitored, checked, and reevaluated in an ongoing process involving supercomputers, caseworkers, fraud control agents, grocers, and neighbors."[20] If the Constitution really

14 Julia Angwin, Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance (2014).

15 Matt Sledge, *Alex Kozinski, Federal Judge, Would Pay $2,400 a Year, Max, for Privacy*, Huffington Post (Mar. 4, 3013), http://www.huffingtonpost.com/2013/03/04/alex-kozinski-privacy_n_2807608.html.

16 *United States v. Pineda-Moreno*, 617 F.3d 1120, 1123 (2010) (Kozinski, C. J., dissenting from denial of rehearing en banc).

17 *United States v. Jones*, 132 S. Ct. 945 (2012); *see also Grady v. North Carolina*, 135 S. Ct. 1368 (2015).

18 *United States v. Pineda-Moreno*, 591 F.3d 1212 (2010), *cert. granted, vacated* 132 S. Ct. 1533 (2012).

19 *Pineda-Moreno*, 617 F.3d at 1123.

20 John Gilliom, Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy vii-viii (2001).

does not distinguish between wealthy and poor, shouldn't it protect welfare recipients as much as anyone else?

Even the super rich don't always have consent as an option. Setting aside apps that steal personal data without notice, such as Brightest Flashlight, some services just need your data to function. Google Maps can't give you directions without knowing where you are. Social networking sites only work if you reveal something about yourself. Your cell phone needs to know where you are to connect to the nearest cell towers, and because the FCC requires cell companies to be able to locate you for 9-1-1 emergency response.

Even for several services that don't require personal data, escaping the corporate dragnet is well-nigh impossible. Driving an older car with no navigation system shouldn't require anyone to know your whereabouts, but there's no way to avoid the companies that scan your license plates. Taking steps to protect your privacy is often ineffective. Suppose you invest in a privacy-sensitive email client. The provider may encrypt everything you've saved in its databases and promise to collect no information about you. But it cannot make promises on behalf of the email clients your friends and colleagues use. Google, for example, can and probably does scoop up any messages you send to anyone with a Gmail account, regardless of which service you use. With that, Google can fashion your marketing profile.

The bottom line is that, even with all the money in the world, the best chance you have of avoiding the corporate dragnets is to become a cash-carrying, libertarian luddite, in other words, Ron Swanson.[21] For most of us, Soviet citizens had about as much choice.

## IV Laws Limiting Corporate Informants (or, the Lack of Them)

There's very little to stop corporations from turning your data over to the government. The law, as it currently stands, certainly isn't getting in the way. To get its hands on the sort of data corporations have, the Fourth Amendment would usually require the government to get a warrant, backed up with "reasonably trustworthy information" that the data will turn up evidence of crime.[22] But there's a rule-swallowing exception – the third-party doctrine – "A person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[23] Under this doctrine, any information you reveal to a third party doesn't get Fourth Amendment protection; the government can just take it.

The implications of the third-party doctrine in the modern age are tremendous. Every email we send, every website we visit, every file we store in the cloud, every phone call we make utilizes the software and hardware of third parties: servers, satellites, cell towers, etc. It's far from clear that we "voluntarily" expose all this data to these third parties in any conventional sense of the term. But the legal sense is not always the common sense. The Supreme Court has applied the doctrine to banking and phone call records,[24] so

[21] *Parks and Recreation: Gryzzlbox* (NBC television broadcast Jan. 27, 2015) ("We need to talk.... This is a flying robot I just shot out of the sky after it delivered a package to my house.... The package was addressed to my son – who is four years old, and does not own a Gryzll [data mining company] doodad. Somehow the robots looked at Diane's computer and learned something about my child and then brought him a box of presents, so I destroyed the robot").

[22] *Brinegar v. United States*, 338 U.S. 160, 175–76 (1949).

[23] *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979).

[24] *See Smith v. Maryland*, 442 U.S. 735 (1979) (phone records); *United States v. Miller*, 425 U.S. 435 (1976) (bank records).

there's a natural extension to email, search engines, and cloud servers.[25] As a result, the vast majority of government information requests to companies such as cell phone carriers don't need a warrant; a subpoena with no judicial review will often suffice. These give your data very little protection.[26]

The statutory framework that developed post 9/11 has exacerbated the situation. Shortly after the attacks, Congress passed the USA PATRIOT Act, which amended the Foreign Intelligence Surveillance Act by weakening restrictions on domestic surveillance by the government. The text now seems to permit domestic surveillance so long as foreign intelligence gathering is a "significant purpose"; previously, it had to be "*the* purpose."[27] Section 505 of the PATRIOT Act, as interpreted by the National Security Agency (NSA), allows the NSA to send "national security letters" to corporations, complete with gag orders, demanding the records, files, emails, etc., of their customers. Such requests typically require no warrant and receive no judicial review. Only one in every five thousand or so does require a warrant. The secretive Foreign Intelligence Surveillance Court (FISC) reviews these warrants and overwhelmingly approves them, rejecting just .03 percent.[28] This is hardly surprising, given that the warrant applications are *ex parte* and rarely see the light of day through, for example, a criminal trial.

In addition to issuing subpoenas for information about specific individuals, the government enlists corporations in mass domestic surveillance programs. In 2002, Department of Defense Admiral John Poindexter set about developing the Total Information Awareness (TIA) program. Its purpose was plain from its name – to know *everything*. More specifically, it sought to do this with help from the companies that transmit our electronic communications. In the words of one *New York Times* correspondent, TIA was "determined to break down the wall between commercial snooping and secret government intrusion."[29] But even the name was too evocative of Big Brother for most members of Congress. TIA was formally defunded. Behind the scenes, though, it was broken into several separate programs and continued under different names using black budgets. Today the program is thriving through the data gathering and mining operations of the NSA. Edward Snowden drew attention to some of these programs, such as PRISM

[25] One court has held that the third-party doctrine would not necessarily compromise Fourth Amendment protections of the content of emails when the government tries to compel an Internet service provider to turn them over. *See United States v. Warshak*, 631 F.3d 266 (2010). But between metadata and material ISPs may turn over voluntarily, there's not much need for the content anyway.

[26] Daniel J. Solove, Nothing to Hide 93 (2001). There are some statutory protections for email and phone records, *see e.g.* Stored Communications Act, 18 U.S.C. § 2702 (2012), but these are changeable and do not provide the level of security ensured by the Fourth Amendment. Stephen J. Schulhofer, More Essential than Ever, 128 (2012). For example, under the Stored Communications Act, the government can obtain record and content information (more than six months old) from electronic service providers by clearing a "reasonable grounds" bar. Stored Communications Act § 1703(d). The Fourth Amendment's probable cause requirement is more demanding.

[27] USA PATRIOT Act, Pub. L. No. 107–56, § 218, 115 Stat. 272 (2001) (amending Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1804(a(7)(B), 1823(a)(7)(B)) (emphasis added). *But see* In re Sealed Case, 310 F.3d 717, 735–36 (FISA Ct. Rev. 2002)

[28] Colin Schultz, *The FISA Court Has Only Denied an NSA Request Once in the Past 5 Years*, Smithsonian (May 1, 2014), http://www.smithsonianmag.com/smart-news/fisa-court-has-only-denied-nsa-request-once-past-5-years-180951313/?no-ist; Erika Eichelberger, *FISA Court Has Rejected .03 Percent of all Government Surveillance Requests*, Mother Jones (June 10, 2013), http://www.motherjones.com/mojo/2013/06/fisa-court-nsa-spying-opinion-reject-request.

[29] William Safire, *You Are a Suspect*, N.Y. Times (Nov. 12, 2002), http://www.nytimes.com/2002/11/14/opinion/14SAFI.html.

(which collects Internet data) and MAINWAY (which collects phone call data). Some of these programs were approved using the processes, such as they are, set in place by FISA; others were not. As to the other ways the NSA accesses the data corporations collect on us – we don't know what we don't know.

## V A Change Is Warranted

You don't need to be a privacy nut or an anarcholibertarian to see that there's a problem here. Nor do you need to have lived in a totalitarian surveillance state, surrounded by private informants, to see the frightening potential of the corporate–government intelligence alliance. It's no coincidence that the United States is the only country in the West without fundamental data protection laws.[30] Europe, which has firsthand experience with surveillance states using private informants, is well ahead of the curve in giving consumers enhanced control over their data.[31] People like Professor Orin Kerr, who say the current regime in the United States just levels the playing field between the government and sophisticated criminals, must be wrong.[32] The concern is not about how surveillance affects criminals, but about how it affects the rest of us.[33] Reflecting on the problems with private informants in totalitarian regimes can help frame the search for a solution that could work in the United States.

The problem in the Soviet Union was not that private parties knew what you were doing. Ordinary social interaction is impossible without revealing personal information to others. Pavel Morozov couldn't have had a meaningful relationship with his father had the two not shared important facets of their private lives. The trouble begins when the government strongly incentivizes private associates to snitch on each other. In that environment, the sort of interpersonal confidences needed for individual autonomy disappear.

Similarly, there's nothing inherently troubling about private corporations collecting data on us. Scholarly calls to impose hard limits on what data corporations can collect or how long they can store it are misplaced.[34] We like our free apps and lower-cost cell phone service, and these are only possible when data sales and advertising can help cover the developers' overhead. Not all of us can afford to pay out-of-pocket for the suite of social, entertainment, and productivity software we have on our phones. For those of us with limited disposable income, data collection gives us more options, not fewer; we can trade our data, which we have, in place of money, which we may not. Although studies show two-thirds of Americans say they don't like being tracked by corporations online, everyone likes the free apps such tracking supports. No one likes spending money either, but everyone likes what he gets in return.

30 Schneier, *supra* note 12, at 200; Pauton & Claypoole, *supra* note 2, at 232 ("How did the impulse to treat privacy as a human right arise in Europe, and not in the United States? … Much of Europe is not more than a generation or two from fascist or communist dictatorships, in which the government strove to know all the secrets of its citizens").

31 *See, e.g.*, Commission Regulation (EU) 2016/679 of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1.

32 Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 Mich. L. Rev. 561 (2009).

33 *See* David Gray, The Fourth Amendment in an Age of Surveillance (2017).

34 One such call comes from Pauton & Claypoole, *supra* note 22, at 234–36.

Of course, there should be *some* limits on data collection. Norms of consent should govern to the extent possible. That will require corporations to be more forthcoming about what data is collected and how it is used. Shorter, simpler, and more transparent privacy policies would go a long way toward helping customers understand what "I Agree" really means. Many American companies are already complying with such transparency requirements in order to do business in Europe. The Department of Commerce runs a program that registers companies as Safe Harbor Compliant, meaning, in part, that they follow Europe's more stringent data transparency laws. Bringing the same norms to bear in the American market shouldn't be very troublesome. While there may also be uses that should be disallowed even with customer consent (Facebook's confessed manipulation of customer emotions comes to mind),[35] freedom of contract should be the strong default.

As with individual informants, corporate data collection begins to raise serious problems when government access to that data enters the picture. The worst corporations can usually do on their own with our data is lure us into purchasing products we may not need; they can't throw us into jail; that's the sole prerogative of the government. The possibility that the information we expose to corporations may make its way into government hands has uniquely chilling effects. In the words of Chief Justice Warren Burger, "When an intelligence officer looks over every nonconformist's shoulder in the library, or walks invisibly by his side in a picket line, or infiltrates his club, the America once extolled as the voice of liberty heard around the world no longer is cast in the image which Jefferson and Madison designed, but more in the Russian image."[36] Ditto for nonconformists' email accounts, phone calls, and electronic files.

We need to balance corporate interests in data collection, government interests in law enforcement, and individual interests in privacy. Thinking through how to strike the right balance, we need to reflect on the ways government induces private parties to turn over our data. The Soviet Union recruited its informants with both carrots and sticks, and the same is true of how the U.S. government gets information about us from corporations. Let's talk about the sticks first. As discussed, the government has easy access to customer information under the PATRIOT Act and FISA. And it *should* have some sort of access. That's how it keeps us safe from terrorists and other criminals. But the level of access should be balanced against Fourth Amendment civil liberties with an eye to what actually works.

One thing that doesn't work: dragnet style surveillance à la PRISM and MAINWAY. There is little to no evidence of its effectiveness. From a mathematical standpoint, the problem is one of data overload. Dragnet systems pull in a ton of information. Advanced searching algorithms can help to an extent and may work well for mundane criminal activity. But the sort of criminals the dragnets are meant to catch, such as terrorists, don't fit into well-defined profiles. Algorithms that try to pick out potential criminals on the basis of profiles are unworkable since they overwhelm the system with false positive results.[37] In 2014, the Privacy and Civil Liberties Oversight Board, appointed by President

[35] Vindo Goel, *Facebook Tinkers with Users' Emotions in Newsfeed Experiment, Stirring Outcry*, N.Y. Times (June 29, 2014), http://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html.

[36] *Laird v. Tatum*, 408 U.S. 1 (1972).

[37] Schneier, *supra* note 12, at 136–40.

Obama, found no evidence that mass surveillance of telephone calls ever made a significant security contribution. "We have not identified," the Board wrote, "a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation."[38]

If dragnet surveillance is out, that leaves us with targeted surveillance, as when the NSA asks a cell carrier to provide location data on a single customer. Under current law, a subpoena will do the trick. But here's something curious: If the government were to get the same information using costlier old-school techniques, such as tailing or GPS locators, the Fourth Amendment would require it to get a warrant. This makes no sense. Why should the government have to go to a judge for a warrant to follow someone on foot at a cost of $275/hour but just present a subpoena to get cell-tracking data for one-thousandth the price?

We may be in one of those transitional points when the law has to catch up to technology and common sense. In the early part of the twentieth century, wiretapping was the new technology. In 1928, the Supreme Court first considered whether police wiretapping counted as a "search" and so whether the Fourth Amendment applied to it. The Court decided it did not, since wiretapping doesn't involve any sort of physical intrusion: "There was no entry of the houses or offices of the defendants."[39] Justice Brandeis, in dissent, saw the danger of the precedent, but was unable to persuade his colleagues:

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.... Can it be that the Constitution affords no protection against such invasions of individual security?[40]

It was forty more years before the implications of the ruling became fully apparent to a majority of the Court. In 1967, the Supreme Court reversed course. In doing so, it developed a more refined understanding of the Fourth Amendment: It protects "reasonable expectations of privacy" rather than just physical boundaries.[41]

Today, the conceptual sticking point is not privacy as it relates to physical intrusions, but privacy as it relates to third parties. Under current law, there can be no reasonable expectation of privacy, and so no Fourth Amendment protections, for information one person reveals to another. That may make enough sense if you're speaking loudly to the guy seated beside you on a crowded subway. Then you truly have forfeited your privacy. But there's an obvious difference when you're speaking in your own home, and the "third party" is a cell company algorithm logging the call. Hopefully it won't take us forty years to catch on. At least one member of the Supreme Court, Justice Sotomayor, is already hot on the trail.[42]

[38] Privacy & Civil Liberties Oversight Bd., *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (Jan. 23, 2014), https://fas.org/irp/offdocs/pclob-215.pdf.

[39] *Olmstead v. United States*, 277 U.S. 438, 464 (1928).

[40] *Id.* at 474 (Brandeis, J., dissenting).

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

[42] *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a

Some scholars, such as Stephen J. Schulhofer, have proposed alternative conceptions of privacy that might do the trick. He argues that privacy is not really about keeping information secret from third parties. Information we share with our spouses, friends, and doctors is private, even if it's no longer totally secret. Schulhofer suggests that privacy is about having control over our information rather than keeping it secret.[43] Though he needs to do some line drawing (if you tell everyone except your spouse about an affair, have you still kept it private?), Schulhofer may be headed in the right direction. He argues that, at least with respect to corporations that provide services for which customers have no realistic alternative, the government should need a warrant to force corporations to turn over customer data.

Perhaps because he didn't have in mind the fuller history of using private informants, Schulhofer's proposal doesn't go far enough. Not all informants in the Soviet Union were compelled to talk. Many willingly pointed fingers at neighbors, sometimes out of a sense of duty; but surely just as often they did it to collect financial rewards. As documented earlier, the same happens in the United States; providing information to the government can be very lucrative for corporations.

Now let's talk about the carrots the government offers private informants. How do we limit corporations from voluntarily revealing to the government what they know about us, often for profit? Laws directly barring corporations could bump up against complications with the First Amendment freedom of speech.[44] Some commentators have suggested that intervention may not be necessary. Perhaps free market forces will take care of matters as consumers become more interested in the privacy of their data. There is some evidence that these forces are pushing a few corporations to get serious about privacy. Several large tech companies have announced, for example, that they will violate the gag orders attached to national security letters and tell customers when the government requests their data.[45] Google, among others, has also started publishing bulk statistics on data requests it receives.

But protecting consumer data is too important to leave to the whims of market forces. However warm and fuzzy Google or Apple may make us feel when it promises to tell us about national security letters or to protect our encrypted data, they are still for-profit corporations. Warm and fuzzy isn't their modus operandi; profit is. The winds of increased market share may tell one day in favor of privacy, and another against it. We should not forget that the same Google that will tell us today whether the government is poking

great deal of information about themselves to third parties in the course of carrying out mundane tasks" [internal citations omitted]).

43 Schulhofer, *supra* note 27, at 8–9; *see also* Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 Miss. C.L. Rev. 227, 229–33 (2012) (offering a similar definition of "privacy," which became the benchmark for the American Bar Association's Criminal Justice Standards on Law Enforcement Access to Third Party Records).

44 Though no corporations have, so far as we know, raised such First Amendment objections yet.

45 Craig Timberg, *Apple, Facebook, Others Defy Authorities, Increasingly Notify Users of Secret Data Demands after Snowden Revelations*, Wash. Post (May 1, 2014), https://www.washingtonpost.com/business/technology/apple-facebook-others-defy-authorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html. The Electronic Frontier Foundation has ranked companies on how often they notify users about such demands. Marcia Hoffman et al., *2012: When the Government Comes Knocking, Who Has Your Back?*, EFF (May 31, 2012), https://www.eff.org/files/who-has-your-back-2012_0_0.pdf.

around about us was arguing in favor of the third-party doctrine in court yesterday.[46] And the day before that had a CEO who would proclaim, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[47] Even if you do trust Google to do right by you, can you trust hundreds of other companies, such as Acxiom, who collect your data behind the scenes and have little interest in your goodwill?

## VI Corporate Instruments of State

If we can't directly prevent corporations from turning over our data, and we can't trust them to limit themselves, we need some way to place restrictions on the other party in the transaction: the government. The Fourth Amendment was designed to rein in the government anyway, not corporations. The usual way the Fourth Amendment limits the government is by forcing it to get a warrant before searching us. To get a warrant, it has to persuade a judge that there's a good chance the search will turn up some evidence of crime. Something like a warrant requirement might do the trick here too. But there's a snag: Under current doctrine, the government could only possibly need a warrant if it is *compelling* a corporation to turn over data. What we're talking about now is how to restrict corporations from *voluntarily* (usually in exchange for cash) turning over our information.

There's conceptual space for requiring the government to get a warrant before it even *requests* customer data from corporations. Then the government would have to convince a judge that there's some likelihood the request will turn up evidence of crime before it can send the request. The practical effect of this would be that the government would have to get a warrant before a corporation could voluntarily provide our data. Without a warrant, the government could not make a request for data. And without a request, the corporation wouldn't know what to send. This would make the government's legal burden for getting, e.g., location data on a customer from a cooperative cell phone company just as high as getting authorization to put a GPS tracker on the same customer's car.

But is there legal space for a warrant requirement for data requests? The executive branch could voluntarily abide by the requirement, or a similar sort of restriction. After all, the executive branch has the power to establish internal norms governing investigations. But we shouldn't hold out for that to happen anytime soon. Snowden's revelations in 2013 showed just how data hungry the executive branch is.

Passing new laws might be another approach to getting the warrant requirement for data requests. We've been talking about "the government" as though it were a unitary entity. In fact, there are three branches, and they don't always see eye to eye. A privacy-friendly Congress might try to pass some statutory limits on data requests. But doing so would be risky. All of the three branches have constitutionally designated domains,

[46] Paul Calahan, *Google: Gmail Users Can't Expect Privacy When Sending Emails*, Independent (Aug. 14, 2013), http://www.independent.co.uk/life-style/gadgets-and-tech/news/google-gmail-users-can-t-expect-privacy-when-sending-emails-8762280.html ("Just as a sender of a letter to a business colleague cannot be surprised that the recipient's assistant opens the letter, people who use Web-based email today cannot be surprised if their emails are processed by the recipient [email] provider in the course of delivery").

[47] *Google CEO on Privacy (VIDEO): 'If You Have Something You Don't Want Anyone to Know, Maybe You Shouldn't Be Doing It'*, Huffington Post (Mar. 18, 2010), http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html.

and they're not supposed to overstep their bounds. It's the executive branch that has the authority and discretion to direct investigations. If Congress tried to meddle, it might find itself butting heads with an executive branch keen to guard its turf.

No branch of government can violate the Constitution, even when exercising one of its constitutionally designated powers. So if there's little hope of the executive restricting itself, and separation of powers or political problems with Congress trying to do it, constitutional limits on the executive branch might do the trick. Congress wouldn't have to get involved, just as it didn't when the Supreme Court found that the Constitution requires the executive branch to get a warrant before attaching GPS trackers. The only problem is that the current understanding of the Fourth Amendment, and the third-party doctrine in particular, cuts against a warrant requirement for data requests.

Or does it? The third-party doctrine is not absolute. It doesn't treat all third parties alike. Some differences are irrelevant for purposes of the Fourth Amendment. For example, it's probably beside the point how much information the third party collects. Corporations collect much more information than natural persons, but the third-party doctrine applies regardless of how sophisticated the third party is at persuading you to open up. But some differences are extremely relevant, such as whether or not the third party is really an "instrument of state."[48] When a third party is acting at the direction or encouragement of the government in collecting information or investigating possible crime, the third party is considered an instrument of the state. Since instruments of state are basically operating as agents of the government, the third-party doctrine doesn't apply – there are still effectively just two parties, the government and the target of the investigation. So the protections of the Fourth Amendment remain in full force.

Admittedly, the typical instruments of state recognized by the Supreme Court don't look much like huge corporate data mongers. Mostly they're just ordinary individuals, like airline employees who open a customer's luggage looking for drugs. But there's no reason that corporations couldn't also be considered instruments of state.[49] Indeed, in light of the tight public–private intelligence partnership discussed previously, there may be very good reasons a lot of them should be. Courts consider two factors when determining whether someone is an instrument of state: 1) the degree of government involvement, knowledge, or acquiescence, and 2) the intent of the party conducting the search.[50] As with any multifactor, balancing test, most scenarios fall in a "gray" area and need individualized consideration.

The argument for treating data-gathering corporations as instruments of the state is stronger in some cases than in others. Consider cell phone companies collecting location data. The government's level of involvement, knowledge, and acquiescence in collecting that data is extremely high. As mentioned, a government agency, the FCC, even requires cell phone companies to track customers. As to the intent of the cell companies,

48 *Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971).

49 David Gray and Danielle Citron take a first step in this direction, but limit their discussion to the most sweeping corporate data collectors. David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 Minn. L. Rev. 62, 133–43 (2013). It is important that a corporation can qualify as an agent of the state whether it collects "limited" or "broad and indiscriminate" information. *Cf. id.* at 143. Corporate and government entities can cheaply aggregate limited information to end up with the equivalent of broad and indiscriminate information.

50 *United Sates v. Walther*, 652 F.2d 788 (9th Cir. 1981).

part of their motive is surely commercial profit from selling the location data to marketers. But another substantial motive must be complying with FCC regulations and, at the same time, profiting from selling location data to the government. Both factors tell pretty strongly in favor of treating cell phone companies as instruments of state when they collect customer location data. So there's a good argument that the third-party doctrine shouldn't apply in such a case, and some sort of warrant requirement should intermediate the government's access to that data.

The argument may be not be quite as strong with information such as email metadata or Kindle reading habits. These are different from cell phone location data in that there is no government mandate that corporations collect the data and no immediate revenue stream (that we know of) from the government to the corporation for that information. But even if government agencies aren't directly involved in gathering the customer data, they certainly know about it and acquiesce to it. As to the second factor, third party intent, the overriding incentive corporations have for collecting the data is, without a doubt, commercial. But the wheels of commerce travel far, and we know government agencies are one of the downstream purchasers (if not sometimes a direct purchaser) of this data. At a minimum, part of the revenue stream the corporations enjoy from collecting this sort of data is due to government sales. Corporations collecting this sort of data are in the gray area for identifying instruments of state. As a consequence, so are possible Fourth Amendment protections under this analysis.

Corporate instruments of state differ in another respect from typical instruments of state – they'd collect our information even without government prompting. We can't just tell them to stop without sacrificing all the social benefits that result from collecting and marketing this data. We also can't just tell them never to talk to the government, since there are cases when the government has a legitimate interest in consumer data. What's needed is for corporations to be more sophisticated in how they segregate and share data they collect. Corporations should implement internal controls to ensure that customer data is never shared with the government, unless it is subject to a legitimate request. Other downstream entities to which the corporation sells data would need to implement the same controls. This may sound like a tall order. But it should be a walk in the park compared to the complex data management that already goes into complying with laws that protect customer health and financial information.

The analogy to customer health data protections raises another provocative possibility – giving consumers private remedies against corporations that improperly turn their data over to the government. While the Health Insurance Portability and Accountability Act,[51] which protects health data, provides no private right of action, some state laws do. Perhaps something similar could be done to enable consumers to protect their privacy interests against corporations that are too cozy with the government.[52] Giving corporations some skin in the game and empowering a citizenry of private enforcers will surely help the government stay within Fourth Amendment bounds when requesting data.

[51] Pub. L. No. 104–91, 110 Stat. 1936 (1996).

[52] Kiel Brennan-Marquez has one interesting proposal about how to do this that involves treating corporate data collectors as "information fiduciaries." Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 Fordham L. Rev. 611 (2015).

## Conclusion

The United States is not a totalitarian state. The Soviet Union was, in large part because it had the capacity, if not to monitor all aspects of everyone's life, to raise an omnipresent fear of being monitored through its use of private informants. But it's not for nothing that William Binney, a former NSA official, could gesture with a single hand and say, "We [Americans] are, like, that far from a turnkey totalitarian state."[53] The infrastructure for a potential surveillance state is in place, and it is largely in private hands. If this worries us (and it should), we need to think about the unique complications, legal and philosophical, that private informants raise. The third-party doctrine, which currently gives the government easy access to any information that passes through the private infrastructure, is dangerously outdated. We have suggested one possible way to rein it in, by treating many corporations with access to customer data as instruments of state. Maybe it works. If not, we sure hope someone else figures out something sensible.[54] Nothing short of the freedoms that define us as Americans, not to mention the next free-play release of Angry Birds, are at stake.

[53] James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, Wired (Mar. 15, 2012), https://www.wired.com/2012/03/ff_nsadatacenter/.

[54] The Electronic Privacy Information Center (EPIC) has made substantial inroads into this many-headed problem for more than twenty years from legal, political, and technical fronts. To read about some of its cutting-edge, interdisciplinary work in the area, see Privacy in the Modern Age: The Search for Solutions (Marc Rotenberg et al. eds., 2015).