RESPONSE

COMMUNICATIONS PRIVACY FOR AND BY WHOM?

RYAN CALO†

In response to Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373 (2014).

INTRODUCTION

Professor Orin Kerr has proposed an elegant new thought experiment in his piece, *The Next Generation Communications Privacy Act*.[1] The Article efficiently relays the history and structure of the Electronic Communications Privacy Act of 1986 (ECPA),[2] a law that "grants Internet users a set of statutory privacy rights that limits the government's power to access a person's communications and records."[3] The Article then ably diagnoses what is wrong with ECPA today—namely, that changes in technology and constitutional law over the last quarter century have rendered ECPA outdated.[4] Finally, the Article proposes four plausible principles to guide Congress were it to write a new electronic communications privacy statute

† Assistant Professor of Law, University of Washington School of Law; Faculty Director, Tech Policy Lab, University of Washington; and Affiliate Scholar, Stanford Law School Center for Internet and Society. Thank you to Susan Freiwald, Jennifer Granick, and Peter Winn for their thoughts, and to the Gallagher Law Library at the University of Washington for helpful research assistance.

1 Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373 (2014).

2 Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

3 Kerr, *supra* note 1, at 375, 378-90.

4 *Id.* at 376-77, 390-410.

from scratch, rather than reform ECPA at the margins, as contemporary advocates propose.[5]

Professor Kerr's argument is clear, forceful, and fundamentally sound in the sense that his conclusion follows from his premises.[6] The Article also makes a series of quiet assumptions, however, that readers may find controversial.

First, the Article reads as though ECPA exists only to protect citizens from public officials. According to its text and to case law, however, ECPA also protects private citizens from one another in ways any new act should revisit.[7] Second, the Article assumes that society should address communications privacy with a statute, whereas specific experiences with ECPA suggest that the courts may be better suited to address communications privacy—for reasons Professor Kerr himself offers.[8] Finally, the Article addresses ECPA in isolation from the Foreign Intelligence Surveillance Act of 1978 (FISA),[9] which seems strange in light of revelations that our government systematically intercepts and stores its citizens' electronic communications under FISA's auspices.[10]

Put another way, *The Next Generation Communications Privacy Act* succeeds marvelously on its own terms, but not necessarily on everyone else's. Worse still, we do not benefit from Professor Kerr's powerful insights regarding the issues he omits.

I. WHY THE STATE?

The Next Generation Communications Privacy Act proceeds throughout as though ECPA's exclusive purpose is to protect citizens from public officials.[11]

---

5 *Id.* at 377-78, 411-18.

6 There is room to quibble here and there. A person with a greater taste for privacy might argue that some "noncontent" information (e.g., that a person traveled to or called an abortion clinic) should be protected to the same degree as "content" (e.g., what that person says to the clinic). *But see id.* at 398-401 (distinguishing treatment of "noncontent metadata" from "the contents of communications"). A technologist might contend that improvements to search algorithms were just as relevant as cheaper storage in creating contemporary surveillance capabilities. More practically minded readers might find "major principles," *id.* at 378, less useful than model language or specific details of a proposal—where devils sometimes live. The focus of this Response is elsewhere.

7 *See infra* Part I.

8 *See infra* Part II.

9 Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended in scattered sections of 18 U.S.C. and 50 U.S.C. §§ 1801–1811 (2006)).

10 *See infra* Part III.

11 *E.g.*, Kerr, *supra* note 1, at 375, 380, 383-84, 387, 394, 402, 408 (focusing on how ECPA "limits the *government's* power to access a person's communications and records" (emphasis added)). *But see infra* note 15.

One could easily read the entire Article without realizing that ECPA also protects citizens from one another. Yet ECPA by its text disallows any unauthorized party—not just government officials—from intercepting or accessing private electronic communications.[12] Indeed, a number of prominent ECPA cases involve surveillance activity by nongovernmental private parties, such as employers, litigants, and web-monitoring companies.[13]

Professor Kerr's omission matters for a few reasons. First, where solely private actors are concerned, changes in how courts interpret the Fourth Amendment neither furnish a reason to revisit ECPA[14] nor create a constitutional floor for privacy violations should ECPA prove inadequate.[15] Second, the "plummeting costs of storage"[16] present as many questions in private surveillance as in public surveillance. Does it still make sense, for example, for the Stored Communications Act[17] to allow Internet companies voluntarily to disclose any amount of noncontent information to nongovernmental entities?[18] Similarly, what is consent to "intercept" in a world

---

12 *See* 18 U.S.C. § 2511 (2012) (placing prohibitions on "any person," rather than on government entities or officials); *id.* § 2701 (authorizing punishment for "whoever" unlawfully accesses stored communications).

13 *E.g.*, Theofel v. Farey–Jones, 359 F.3d 1066, 1072-77 (9th Cir. 2004) (finding an ECPA violation in private litigants' use of an unlawful subpoena); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113-15 (3d Cir. 2004) (applying ECPA to an employment dispute in which the employee asserted that his employer improperly accessed his email account); *In re* Pharmatrak, Inc., 329 F.3d 9, 21-22 (1st Cir. 2003) (finding that a web-monitoring company "intercepted" personal information and thus violated ECPA's prohibitions); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874-80 (9th Cir. 2002) (applying ECPA to an employment dispute in which an employee sued his employer and alleged that the employer accessed the employee's website under false pretenses). For another example, just last year, plaintiffs filed a class action lawsuit alleging that Google's practice of scanning emails in furtherance of its advertising purposes violates ECPA. *See* Plaintiff's Consolidated Individual & Class Action Complaint at 1-5, *In re* Google Inc. Gmail Litig., No. 13-2430 (N.D. Cal. Oct. 1, 2013), 2013 WL 5823090.

14 *Contra* Kerr, *supra* note 1, at 376-77 (suggesting that where "new principles of [Fourth Amendment] constitutional law have emerged," ECPA's coverage must also change); *id.* at 399-401 ("[R]ecent Fourth Amendment rulings suggest that the focus of the statute can turn more to noncontent information . . . that remain[s] outside the Fourth Amendment.").

15 Professor Kerr acknowledges in passing that "[s]tatutory protections are still needed to regulate nongovernmental access to contents of communications that the Fourth Amendment will not reach," yet comments on neither what the protections should be, nor whether the next generation of ECPA is the right place for them. *Id.* at 400.

16 *Id.* at 376.

17 ECPA, tit. 11, 18 U.S.C. §§ 2701–2711 (2012).

18 *See generally id.* § 2702(c)(6) (allowing electronic communications providers to divulge their subscribers' records to "any person other than a governmental entity").

where consumers may click through a dozen terms of service in a day?[19] Were Congress to accept Professor Kerr's invitation to rewrite ECPA, it would receive little guidance about how to address these and related issues of private access.

II. WHY A STATUTE?

The premise of *The Next Generation Communications Privacy Act* is that decreases in digital storage costs, coupled with new clarity regarding how the Fourth Amendment applies to electronic communications, suggest the need to revisit the 1986 statute. Rather than tinker at the margins, as others have suggested,[20] Professor Kerr would rewrite the law from scratch.

I admire Professor Kerr's "blue sky" approach, but it does beg a question: If we are starting over anyway, why not use a different approach entirely—such as a better interpretation of the Fourth Amendment?

In other work, Professor Kerr expressly defends the use of statutes over constitutional interpretation to address information privacy concerns.[21] His preference for writing another ECPA makes sense in this light. Professor Kerr's views generated debate at the time,[22] and I acknowledge a certain futility in fighting the same battles anew.[23] Yet our experiences with ECPA represent particularly persuasive examples of why courts may be better positioned than legislatures to address information privacy—for exactly the

---

19 *See generally* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1882-92 (2013) (exploring the challenges consumers face when making important privacy choices).

20 For example, Professor Kerr refers to the Digital Due Process Coalition. *See* Kerr, *supra* note 1, at 386-89 (discussing the Coalition's proposals). The Coalition is a group of advocates, scholars, and industry members urging Congress to amend ECPA in specific ways. *See Who We Are*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163 (last visited Apr. 20, 2014) (announcing the Coalition's goal "[t]o simplify, clarify, and unify the ECPA standards," and listing Coalition members such as Susan Freiwald). *But see* Susan Freiwald & Sylvain Métille, *Reforming Surveillance Law: The Swiss Model*, 28 BERKELEY TECH. L.J. 1261, 1330-31 (2013) (advocating a wholesale rewrite of ECPA based on a Swiss model).

21 *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 838 (2004) ("Additional privacy protections are needed to fill the gap between the protections that a reasonable person might want and what the Fourth Amendment actually provides. . . . Congress will likely remain the primary source of privacy protections in new technologies thanks to institutional advantages of legislatures.").

22 *See, e.g.*, Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 760-77 (2005) (arguing against "pushing the courts aside").

23 Although, as Margaret Thatcher is supposed to have said, you may have to fight a battle more than once to win it.

reasons that Professor Kerr himself develops in suggesting the need for ECPA reform.

Professor Kerr's original argument holds that legislatures have several institutional advantages over courts when regulating information privacy. For instance, legislatures tend to understand technology better than courts.[24] But is this true in the ECPA context? Congress may have understood a snapshot of the technology it was regulating in 1986, but it obviously failed to appreciate the technology's trajectory. Part of understanding technology is appreciating which of its aspects will change as bandwidths or business models evolve.

Legislatures are supposedly better able to keep pace with technological change as well.[25] Yet in the quarter century since it passed ECPA, Congress has never meaningfully updated the statute to reflect an observable sea change.[26] Meanwhile, Professor Kerr openly admits that "[i]n the last five years, courts have begun to settle the basic parameters of how the Fourth Amendment applies to the Internet,"[27] and "Fourth Amendment protections are becoming established in ways that may soon outpace statutory standards."[28]

In other words, Professor Kerr paints a vivid picture of how the courts came to outpace a stagnant statute, and then argues for a new statute that would perpetuate this dynamic. A more comprehensive approach would examine how ECPA reform might halt the progress courts have made in interpreting the Fourth Amendment—a prospect Professor Kerr acknowledges without seeming to appreciate its import for his larger argument.[29]

---

24 *See* Kerr, *supra* note 21, at 858-60 ("Courts tend to be poorly suited to generate effective rules regulating criminal investigations involving new technologies. In contrast, legislatures possess a significant institutional advantage in this area over courts.").

25 *See id.* at 871 ("To ensure that the law maintains its intended balance, it needs mechanisms that can adapt to technological change. Legislatures are up to the task; courts generally are not.").

26 ECPA has been updated about a dozen times since 1986. *See generally, e.g.*, 18 U.S.C. § 2701 note (2012) (Amendments) (listing multiple amendments to one ECPA section, passed as recently as 2002). Yet it has never shed the fundamental dichotomies that, according to Professor Kerr, suggest the need to rewrite the law from scratch. *See generally* Kerr, *supra* note 1, at 390-410 (discussing ECPA's failure to address real-time storage, contemporary forms of Internet communications, noncontent metadata, particularity requirements, and territorial scope).

27 Kerr, *supra* note 1, at 376.

28 *Id.* at 390.

29 *Cf. id.* at 401 (arguing merely that "[e]liminating content protections under ECPA may paradoxically speed up the process of establishing the apparent strong constitutional protections").

III. WHITHER THE NSA?

For the sake of argument, let us assume that ECPA is, at its core, a statute about protecting citizens from the government, and that statutes are the best and most expedient means to do so. There remains the question of whether determining what "electronic communications privacy laws ideally look like"[30] should occur in isolation from a more general inquiry into American surveillance powers and practices.

The Next Generation Communications Privacy Act arrives at an interesting time, amid a series of revelations confirming the extensive—some would say frightening—surveillance activities of the National Security Agency (NSA). According to lawsuits and the press, the NSA intercepts and stores for later analysis literally every communication transmitted across major networks.[31] Meanwhile, the Federal Bureau of Investigation (FBI) also requests and receives phone logs from millions of U.S. citizens under § 215 of the USA PATRIOT Act of 2001.[32] If government officials can already collect and analyze substantial proportions of citizens' electronic communications without a traditional warrant, some readers may wonder whether reforming ECPA is like rearranging the deck chairs on the Titanic.

---

[30] *Id.* at 375.

[31] *See generally* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., PUBLIC HEARING REGARDING THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 123-24 (2014) (statement of Jameel Jaffer, Deputy Legal Director of the American Civil Liberties Union), *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf ("Given the absence of any meaningful limitation on NSA's authority to acquire international communications under Section 702, it's likely that NSA's databases already include the communications of millions of Americans."); JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 22-27 (2014) ("After the 9/11 terrorist attacks, the U.S. government established sweeping, possibly illegal dragnets that captured the phone call and e-mail traffic of nearly every American.").

[32] Pub. L. No. 107-56, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. §§ 1861–1862 (2006)) (authorizing, for counterterrorism investigations and intelligence activities, FBI applications for ex parte orders requiring the production of business records and tangible things). *Cf.* 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 21-56 (2014), *available at* http://www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf ("Under a program authorized by the FISA court pursuant to Section 215, the NSA is permitted to obtain all call records generated by certain telephone companies in the United States."); ANGWIN, *supra* note 31, at 27 (reporting that three days after the attacks of September 11, 2011, the NSA's agency director "approved warrantless interception of any U.S. phone call to or from specific terrorist-identified phone numbers in Afghanistan" and later "expanded the order to cover all phone numbers in Afghanistan"—actions that ultimately "mushroomed into a massive domestic dragnet").

Despite appearances, the two governmental contexts are analytically distinct. The NSA is not the FBI; it is interested, as its name suggests, in national security rather than routine law enforcement. Likewise, FISA is limited to foreign intelligence—even if reporting also suggests that "foreign" is defined somewhat loosely.[33]

The danger in taking a piecemeal approach to surveillance reform, however, is that these two contexts bleed into one another in practice. Take the phenomenon known as "mission creep." Public understanding is incomplete, but it appears that intelligence agencies sometimes share information gathered outside ECPA strictures with domestic law enforcement.[34]

A next generation communications privacy act could more explicitly address today's widely shared concerns over mass surveillance. While offering guiding principles for reformers, we could ask them to draft a new statute that acknowledges how citizens' information can jump contexts and that guards against such an eventuality.

CONCLUSION

The norms of legal scholarship invite authors to determine the scope of their own argument. We are free to "bracket" issues and to set them to one side in order to focus on another concern. At some point, however, an author can leave out too much in pursuit of clarity. *The Next Generation Communications Privacy Act* represents an elegant thought experiment, but at the cost of assuming away some important aspects of communications privacy. Worse yet, the reader cannot benefit from Professor Kerr's keen insights on the topics he omits. I nevertheless enjoyed the Article immensely, recommend it to readers, and look forward to continued dialogue on this important issue.

---

33 *See, e.g.*, Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES (July 6, 2013), http://mobile.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html ("FISA judges have ruled that the N.S.A.'s collection and examination of Americans' communications data to track possible terrorists does not run afoul of the Fourth Amendment . . . .").

34 *See, e.g.*, John Shiffman & Kristina Cooke, *U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013), http://www.reuters.com/assets/print?aid=USBRE97409R20130805 (detailing a program whereby "[a] secretive U.S. Drug Enforcement Administration unit [funneled] information from intelligence wiretaps . . . to authorities across the nation to help them launch criminal investigations of Americans").

Preferred Citation: Ryan Calo, Response, *Communications Privacy for and by Whom?*, 162 U. PA. L. REV. ONLINE 231 (2014), http://www.pennlawreview.com/online/162-U-Pa-L-Rev-Online-231.pdf.