THE YALE LAW JOURNAL FORUM
JULY 15, 2014

Storage Wars: Greater Protection for Messages in Memory

Matthew Sipe

The laws governing stored communication privacy—enacted almost thirty years ago—may finally be updated to reflect contemporary needs, at least in part. The Email Privacy Act,[1] proposed by Representatives Kevin Yoder (R-Kan.), Tom Graves (R-Ga.), and Jared Polis (D-Colo.), would afford greater privacy protections for stored emails, in particular by requiring a warrant for any searches of emails stored for more than 180 days. This represents a small step towards strengthening the meager restrictions on law enforcement's access to stored communications. Stored communications, as discussed in this Essay, are communications acquired by the government after they have been transmitted, as opposed to communications intercepted while in transit. Currently, stored communications are afforded far less privacy protection than communications in transit—a distinction that fails to comport with modern technological reality.

Under current law, stored communications—as opposed to communications in transit—fall "outside the *Berger*, *Katz*, and Wiretap Act core of highest protection."[2] These classic protections—preventing the government from "infring[ing] upon a reasonable expectation of privacy without prior judicial authorization based on a showing of probable cause"—don't apply.[3] Government acquisition of stored communications is in some cases limited by the Stored Communications Act (SCA), but in many circumstances, including "e-mail [accounts] provided by private employers, such as companies and universities," there is "absolutely no protection from government demands."[4] Even where the SCA does apply, a warrant is not required to obtain

1. Email Privacy Act, H.R. 1852, 113th Cong. (2013).

2. PATRICIA L. BELLIA ET AL., CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE 674 (2011).

3. *Id.* at 666.

4. Susain Frewald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA L. REV. 9, 58 (2004); *see also* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 123-24 (3d ed. 2009) (explaining the meaning of "electronic storage" under the SCA).

communications held in storage for more than 180 days,[5] and requirements for prior notice can be postponed repeatedly in 90-day blocks as needed.[6] This Essay argues that many of these weaker protections for stored communications are not justified. It examines some of the ways that law enforcement acquisition of stored communications uniquely threatens privacy and suggests that there should be stronger safeguards against this type of intrusion.

I. STORED COMMUNICATIONS ALLOW THE GOVERNMENT TO APPLY NEW TECHNOLOGY TO OLD DATA

Moore's Law predicted in 1965 that processing power would double approximately every two years.[7] This prediction has proved remarkably accurate,[8] and the growth of computing power seems unlikely to slow in the future.[9] Improvements to search algorithms and data analytics, pursued by the government[10] as well as private entities,[11] also occur at a rapid pace.

As a result of these technological developments, communications data in storage for only a few years can become subject to a level of analysis that may have been inconceivable at the time it was created. Government use of stored communications thus threatens to violate reasonable expectations of privacy by undermining notice. It is fair to say that individuals are on notice that their data are subject to scrutiny from whatever level of technology is contemporaneously available, and that their reasonable expectation of privacy is shaped by that knowledge.[12] It strains credulity, however, to say that

5. 18 U.S.C. § 2703(a)-(b)(1)(B) (allowing the use of administrative subpoenas and court orders in acquiring such communications with prior notice).

6. 18 U.S.C. § 2705(a)(1)-(2) (allowing delays in notice for a variety of reasons, including the possibility of "tampering with evidence" or "jeopardizing an investigation").

7. Gordon E. Moore, *Cramming More Components onto Integrated Circuits*, ELECTRONICS MAG., Apr. 19, 1965, at 114, 115.

8. *See, e.g.*, Jon Stokes, *Understanding Moore's Law*, ARS.TECHNICA (Sept. 27, 2008), http://arstechnica.com/gadgets/2008/09/moore.

9. Kadhim Shubber, *Moore's Law Is Dead: The Future of Computing*, CONNECTIVIST (Oct. 23, 2013), http://www.theconnectivist.com/2013/10/moores-law-is-dead-the-future-of-computing (noting that while transistor technology may be approaching its limits, parallelization, nanotube materials, and quantum computing are posed to take up the slack).

10. *See* TASK FORCE ON NAT'L SECURITY IN THE INFO. AGE, MARKLE FOUND., CREATING A TRUSTED NETWORK FOR HOMELAND SECURITY 6-7 (2003), http://www.markle.org/sites/default/files/nstf_report2_full_report.pdf (noting the spending and research efforts of the NSA, CIA, and TSA, among others, on data analytics).

11. Javed Mostafa, *Seeking Better Web Searches*, SCI. AM. (Jan. 24, 2005), at 66.

12. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) (advancing the idea that technology "not in general public use" is more likely to violate expectations of privacy).

individuals are on notice that future technology—yet unknown and undeveloped—will be retroactively applied to them, and that the prospect of such retroactive application actually factors into their reasonable expectations of privacy.

In particular, advances in technology may cause information that was once considered non-content—i.e., "envelope" information such as recipient, sender, and time—nevertheless to reveal a great deal of information content about a person. For example, innovations in pattern-based data mining might allow the government to draw very accurate and detailed conclusions about an individual's activities despite looking only at the times, places, and recipients of their communications.[13] To the extent that the law seeks to distinguish content and non-content information in terms of communications privacy protection,[14] the government should not be able to circumvent this distinction by using cutting-edge technology on old communications.

II. STORED COMMUNICATIONS REDUCE RESOURCE CHECKS ON POLICE POWER

From the federal government's perspective, stored communications—which have usually already been collected by a private entity—are much more cheaply obtained than intercepting communications in transit. Acquiring communications in transit—whether by pen registers, wiretaps, or bugging—requires the government to expend manpower and money. On the other hand, acquiring stored communications is as simple as requesting a copy. Hence, a lack of protections on stored communications significantly reduces resource constraints on police activity and leaves these communications especially prone to police abuse.

The effects are twofold. First, investigators have reduced incentives to be precise in their searches. With in-transit communications, surveillance over a longer time period or from multiple sources means expending more resources, so that in addition to being constrained by the letter of the law,[15] police have cost incentives to exercise proper discretion. With stored communications, this incentive for self-restraint disappears, leading to deeper and broader

---

13. *See* Ira S. Rubenstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261 (2008).

14. *Compare* Smith v. Maryland, 442 U.S. 735 (1979) *with* Katz v. United States, 389 U.S. 347 (1967). *See generally* BELLIA ET AL., *supra* note 2, at 679 (providing an overview of this distinction).

15. *See, e.g.*, 18 U.S.C. § 2518(1)(d) (requiring that the government specify a time period in applying for a wiretap or bugging, and the sources they will be used on); 18 U.S.C. § 3123(c) (requiring that the government specify a time period in applying for a pen register, and the numbers it will be used on).

surveillance overall. Second, our laws—built on the assumption that police forces have limited resources—factor in the probability that offenders will be caught when determining the length and severity of punishments, in order to ensure sufficient levels of deterrence.[16] If law enforcement has largely unrestricted access to the vast quantity of communications in storage, and there is no commensurate rebalancing of punishment, then the result will be enforcement significantly over the level required for adequate deterrence.

III. STORED COMMUNICATIONS ARE BECOMING INDISTINGUISHABLE FROM COMMUNICATIONS IN TRANSIT

Finally, technological advances have begun to strain the very distinction between communications in storage and communications in transit, if not to render the distinction completely obsolete. Three key ambiguities have already emerged, and will likely multiply in the near future. First, communications are increasingly accessed by front-end clients, obfuscating the issue of when a communication has actually reached its destination. For example, with IMAP or POP protocols, an email client like Microsoft Outlook or Apple Mail downloads a copy of an email from a service provider's storage and either leaves the original (IMAP) or deletes it (POP).[17] If a user never directly accesses the service provider's storage, are his or her communications still in transit until opened via client?

Second, communications are increasingly handled by automated scripts, raising questions of who—or really "what"—can truly be considered the recipient of a communication. For instance, many email and text clients support auto-forwarding triggered by keywords or filters. Does a communication enter storage when it reaches an entirely automated middleman recipient, when the script actually scans it, or when it is forwarded along to a human reader?

Third, more and more data exists in a constant state of motion, with truly static storage taking place only for instants of time. For example, with cloud computing, many networked computers may each contain distributed pieces of a single communication, sending them to each other and receiving them as memory is needed or available on each machine. Does a communication cease

16. *See* Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968).

17. *See IMAP Overview, History, Versions, and Standards*, TCP/IP GUIDE, http://www.tcpipguide.com/free/t_IMAPOverviewHistoryVersionsandStandards-3.htm (last visited July 9, 2014); *POP Overview, History, Versions, and Standards*, TCP/IP GUIDE, http://www.tcpipguide.com/free/t_POPOverviewHistoryVersionsandStandards.htm (last visited July 9, 2014).

to be in transit as soon as it reaches the network, when it is read for the first time, or when (if ever) it actually ceases to be in motion?

All of these questions highlight the extent to which advances in technology blur the distinction between stored and in-transit communications. As line-drawing becomes impracticable, users begin to treat both forms of communication similarly, and their privacy expectations for stored communications begin to match those of in-transit communications. As a result, the privacy protections afforded to stored communications should match those afforded to communications in transit.[18]

CONCLUSION

When the government acquires stored communications, it is able to apply current analysis techniques to data created under outdated expectations, it does so at a dangerously low cost, and it does so by relying on a distinction between stored and in-transit communications that is increasingly impracticable and unrealistic. Greater protections for stored communications are therefore necessary to prevent a significant erosion of privacy rights over the coming years. The Email Privacy Act, while limited in scope, represents a step in the right direction—and evidence of the growing need for stronger privacy protections.

Matthew Sipe is a member of the Yale Law School J.D. Class of 2015. He would like to thank Professor Christine Jolls for her insightful comments and for inspiring an interest in privacy law, as well as the editors of the Yale Law Journal *for their feedback and editorial acumen.*

Preferred Citation: Matthew Sipe, *Storage Wars: Greater Protection for Messages in Memory*, 124 YALE L.J. F. 29 (2014), http://www.yalelawjournal.org/forum/storage-wars-greater-protection-for-messages-in-memory.

18. The further distinction made by the SCA, between communications in "temporary, intermediate" storage, those in "backup" storage, and those in non-backup, post-delivery storage is equally suspect, such that DOJ interpretations, academic analysis, and court opinions already clash and contradict in light of technologic realities. *See* BELLIA ET AL., *supra* note 2, at 676-79.