Information & Communications Technology & Public Policy Project

Science, Technology, & Public Policy Program

Cloud and Mobile Privacy: The Electronic Communications Privacy Act

What Technology Companies Don't Want You to Know

Vivek Mohan

HARVARD Kennedy School

Belfer Center for Science and International Affairs

February 2012

CLOUD AND MOBILE PRIVACY: THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

WHAT TECHNOLOGY COMPANIES DON'T WANT YOU TO KNOW

VIVEK MOHAN
RESEARCH FELLOW, INFORMATION AND COMMUNICATIONS TECHNOLOGY & PUBLIC POLICY

HARVARD Kennedy School
BELFER CENTER for Science and International Affairs

FEBRUARY 2012

Discussion Paper #2012 – 02
Science, Technology, & Public Policy Program Discussion Paper Series

Information & Communications Technology & Public Policy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
Fax: (617) 495-8963
Email: belfer_center@harvard.edu
Website: http://belfercenter.org

This document appears as Discussion Paper 2012-02 of the Belfer Center Discussion Paper Series. Belfer Center Discussion Papers are works in progress. Comments are welcome and may be addressed to the author at vivek_mohan@hks.harvard.edu.

This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the Office of Naval Research.

Copyright 2012 President and Fellows of Harvard College

The authors of this discussion paper invite liberal use of the information provided in it for educational purposes, requiring only that the reproduced material clearly state: Reproduced from Vivek Mohan, "Cloud and Mobile Privacy: The Electronic Communications Privacy Act," Belfer Center Discussion Paper, No. 2012-02, Harvard Kennedy School, February 2012.

Statements and views expressed in this discussion paper are solely those of the author and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

ACKNOWLEDGEMENTS

The author would like to thank Venkatesh Narayanamurti, Benjamin Peirce Professor of Technology and Public Policy, & Director of the Science, Technology and Public Policy Program at the Harvard Kennedy School for his leadership and guidance. Additional thanks go to Zach Tumin, Tolu Odumosu, Aadya Shukla, Michael Sechrist, Lucas Kello, Patricia McLaughlin, Eric Hwang, and Elizabeth Burke for their valuable and thoughtful commentary.

Executive Summary: Consumer expectations of online and mobile privacy have in recent years diverged significantly from reality. In certain circumstances, the United States government has the ability to access a consumer's cloud-based email, location data gathered from their mobile phones, and information about what calls a user places on a mobile device – without a warrant. While a broad coalition is spearheading reform efforts in Washington, providers of these services should take proactive steps to bring consumer understanding of their privacy more in line with reality.

Introduction: A Brief History of ECPA

It is no secret in Washington that the Electronic Communications Privacy Act of 1986 (ECPA)[1] has not aged well. Designed in an era where network computing was more hypothesis than reality, the law amended the Stored Communications Act[2] and the federal Wiretap Statute[3] to preserve a "fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement."[4] Though forward-looking at the time, the past quarter century has seen technology change quite a bit –the statute, however, remains the same, and it is clear that the obsolete wording of ECPA has far outlived its stated goal.

The average consumer in the United States is aware of the advancements that have transformed information and communications technology in the past few decades. Consumers have developed largely reasonable privacy expectations across a wide range of communication platforms – for example, that the government is not able to read their Gmail accounts without a warrant, but that information posted without restrictions on Facebook or Twitter is available for anyone, including the government, to look at. Unfortunately, due to the limitations of ECPA, these expectations are not in line with reality.

Limitations of ECPA

The disconnect between consumer expectation and the legal reality is evinced in three key areas: (1) cloud-based email services, (2) location data gathered from cellular phones, and (3) "transactional data." In each of these areas, the standard for the government to access consumer information is significantly lower than the legally robust requirement of a showing of "probable cause."

While this brief seeks to clearly lay out the real-world implications of ECPA, it is important to understand that there is an inevitable loss of nuance when translating legal doctrine into articulable policy points. The descriptions of ECPA below are intended only as an overview. For a more thorough analysis of the statute, its operation, and its interpretation by various courts, please see "The Electronic Communications Privacy Act of 1986: Principles for Reform" by J. Beckwith Burr.[5] Additionally, as courts around the

---

[1] 18 U.S.C. § 2510 et seq. (2012).
[2] 18 U.S.C. §§ 2701 et seq. (2012).
[3] 42 U.S.C. § 3711 (2012).
[4] House Committee on the Judiciary, Electronic Communications Privacy Act of 1986, H. Rep. No. 99-647, 99th Cong. 2d Sess. 2, at 19 (1986).
[5] J. Beckwith Burr, *The Electronic Communications Privacy Act of 1986: Principles for Reform*, DIGITALDUEPROCESS.COM, HTTP://DIGITALDUEPROCESS.ORG/FILES/DDP_BURR_MEMO.PDF, (last visited Jan. 11, 2011).

country continue to issue decisions that deal with ECPA, this analysis may not reflect current law in all jurisdictions.[6]

I. Cloud-Based Email Services

John uses Gmail for his personal communications, and doesn't delete any of his read mail. Believing that John is engaged in criminal activity, but lacking probable cause, federal law enforcement obtains a subpoena and request for delayed notice (believing John will delete incriminating emails if he finds out), and requires Google to disclose all of John's read email that is more than six months old. Ninety days later, John learns that the government has accessed his Gmail records.[7,8]

The intersection of legal theory and technological advancement has led to a particularly convoluted set of rules that the government must play by when seeking to access email communications. In its most basic form, ECPA protects electronic mail from government surveillance the same way law protects the privacy of paper mail. The government needs a warrant to intercept and read paper mail when it is in transit. If the mail reaches its destination, is opened and read, and stored in a user's house, the government needs a search warrant to retrieve it. However, if the mail is thrown out, the government does not need a warrant to root through the garbage and read the mail.

Initially, these theories made sense when applied to email; however, the analogy has broken down as email has moved to remotely-located storage servers, or 'the cloud.' In the past, a user would log on and download emails from a service provider's remote server to their local machine. The service provider would not keep a copy on their server. Thus, it made sense at the time that electronic storage is defined by law as "temporary, intermediate storage incidental to transmission."[9] However, consumers increasingly use cloud-based email platforms – such as Gmail or Yahoo! Mail – and instead of having their mail deleted from the server, most users choose it as the primary point of storage. The understanding and usage of electronic storage has fundamentally changed in the last 25 years – but the law has not.

---

[6] Federal courts have limited the ability of the government to access cloud based email under a number of theories in some jurisdictions. In 2010, the Sixth Circuit Court of Appeals (which has jurisdiction over Kentucky, Michigan, Ohio, and Tennessee) decided in *US v. Warshak* that such emails were subject to a reasonable expectation of privacy and usage of ECPA as such was unconstitutional. 631 F.3d 266 (2010). However, in most jurisdictions, the analysis presented in the brief represents the current understanding of the courts and the Department of Justice. For more please *see* Burr.

[7] United States Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence Manual*, CYBERCRIME.GOV, HTTP://WWW.CYBERCRIME.GOV/SSMANUAL/03SSMA.HTML, (last visited Jan. 11, 2011).

[8] United States Department of Justice, *Electronic Surveillance Manual – Procedures and Case Law, Forms*, JUSTICE.GOV, HTTP://WWW.JUSTICE.GOV/CRIMINAL/FOIA/DOCS/ELEC-SUR-MANUAL.PDF, (last visited Jan. 11, 2011).

[9] *ECPA Reform and the Revolution in Cloud Computing*, Hearing of the House Judiciary Committee Subcommittee on the Constitution, Civil Rights, and Civil Liberties, JUDICIARY.HOUSE.GOV, HTTP://JUDICIARY.HOUSE.GOV/HEARINGS/PRINTERS/111TH/111-149_58409.PDF, Sept. 23, 2010.

It is beyond the scope of this brief to detail how these antiquated definitions have led to the current application and interpretation of the law. However, the practical implications for users of popular, cloud-based email services such as Gmail are clear:

- As soon as a message is opened, or marked as read, by a recipient, it loses the protection of being in "transmission," and it is likely that the government can access it without a warrant or judicial oversight.[10]
- In most cases, the government does not need a warrant to access messages or attachments that are over 180 days old.[11]

II. Location Data from Cellular Devices

Little understood by consumers is the fact that modern cellular devices produce two distinct kinds of location data. Due to its central role in popular products such as maps and navigation, there is a general public awareness of the existence and operation of Global Positioning System (GPS) chips. A warrant is required for the federal government to access a consumer's GPS data, as it provides latitude and longitude location so precise that it might reveal activities within a constitutionally protected location such as a home.[12]

However, there is another type of location data that cellular devices generate – cell site location data. This data, generated by the cellular phone when connecting to the cell tower, has historically been significantly less precise than GPS location information. Currently, ECPA doctrine holds that such information is sufficiently vague so as to not trigger constitutional protection. This makes it likely that this information can be obtained by the government without a warrant. As cell sites have become smaller and smaller, however, including "mini-cells" that operate within a home or office, the location data generated – and available without a warrant – has in some cases become as accurate as GPS information.[13]

III. "Transactional Data"

Relating to both email and cell phone usage, transactional data includes records of who is calling whom, when and for how long, and records of all the "to" and "from" information associated with one's email, including date, time, and message length. The evolution of technology has seen this information burgeon in quantity and detail. Yet ECPA provides an even more outdated and bizarre standard by which the

---

[10] In this case, there is a delivery of notice is required (either concurrent or delayed) to the affected individual.

[11] Testimony of Associate Deputy Attorney General James Baker, Hearing of the Senate Judiciary Committee: "The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age." April 07, 2011.

[12] Testimony of Associate Deputy Attorney General James Baker, *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age*, Hearing of the Senate Judiciary Committee, HTTP://WWW.GPO.GOV/FDSYS/PKG/CHRG-111SHRG66875/PDF/CHRG-111SHRG66875.PDF at 14, Sept 22, 2010.

[13] Testimony of James Dempsey, *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age*, Hearing of the Senate Judiciary Committee, HTTP://WWW.GPO.GOV/FDSYS/PKG/CHRG-111SHRG66875/PDF/CHRG-111SHRG66875.PDF at 16, Sept 22, 2010.

government can access this information: if a prosecutor files a document with the court stating that such information is relevant to an ongoing investigation, the court *must* issue an order allowing its collection.[14]

Reform Efforts and Policy Recommendations

Part of the reason that these legal standards, despite coverage of the issue by major news outlets, are not widely known, is due to the extremely complicated and interrelated provisions that dictate how the law operates. However, there is blame to be laid at the feet of technology companies who obscure the privacy considerations users should take into account when using their services.[15] Despite the obfuscation, though, these same companies have formed a broad coalition and are making a concerted effort to lobby for updates to ECPA.

I. Digital Due Process Coalition

The Digital Due Process coalition is made up of stakeholders that can be categorized into three major groups: technology companies, civil liberties groups, and trade associations. Among its major members are entities such as the ACLU, Adobe, Amazon.com, AOL, Apple, Center for Democracy and Technology, eBay, Google, HP, IBM, Facebook, Intel, Microsoft, and TechAmerica.[16]

The DDP coalition has identified four major principles that guide their legislative reform efforts. In essence, the principles are as follows:[17]

- The government should need a warrant to access electronic communications not readily accessible to the public.
- The government should need a warrant to access location information from a mobile communications device.
- A judicial review and court finding that there are reasonable grounds to believe "specific and articulable facts…relevant to an ongoing criminal investigation" should be required to access dialed number or email "to and from" information.
- Where the Stored Communications Act authorizes a subpoena to acquire information, a governmental entity may use such subpoenas only for information related to a specified account(s) or individual(s). All non-particularized requests must be subject to judicial approval.

---

[14] J. Beckwith Burr, *The Electronic Communications Privacy Act of 1986: Principles for Reform*, DIGITALDUEPROCESS.COM, HTTP://DIGITALDUEPROCESS.ORG/FILES/DDP_BURR_MEMO.PDF at 19, (last visited Jan. 11, 2011).

[15] Miguel Helft and Claire Cain Miller, *1986 Privacy Law Is Outrun by the Web*, Jan. 9 2011, NYTIMES.COM, HTTP://WWW.NYTIMES.COM/2011/01/10/TECHNOLOGY/10PRIVACY.HTML?_R=4&HP, (last visited Jan. 11, 2011).

[16] Digital Due Process, *Who We Are*, DIGITALDUEPROCESS.ORG, HTTP://DIGITALDUEPROCESS.ORG/INDEX.CFM?OBJECTID=DF652CE0-2552-11DF-B455000C296BA163, (last visited Jan. 11, 2011).

[17] For the list of principles in their original form, please see: Digital Due Process, *Digital Due Process :: Our Principles*, DIGITALDUEPROCESS.ORG,HTTP://DIGITALDUEPROCESS.ORG/INDEX.CFM?OBJECTID=99629E40-2551-11DF-8E02000C296BA163, (last visited Jan. 11, 2011).

The DDP coalition has met with some success in lobbying for ECPA reform. There have been multiple hearings in the House and Senate Judiciary Committees, and in May 2011, Senator Patrick Leahy introduced an ECPA reform bill that incorporates most of the DDP recommendations.[18] However, there has been some pushback – for example, Senate Republicans in September 2010 put out a memo highly critical of both the DDP approach and the implications that reform might have on national security and law enforcement.[19] Even so, prospects for ECPA reform look promising. It bears noting that an oft-repeated maxim, on both sides of the aisle, is that any reform to ECPA must "strike the right balance between privacy and security."[20] It remains to be seen exactly where this balance will be struck.

II. Proactive Education by Technology Companies

While recognizing the effort technology companies have put forth in forming and supporting the DDP coalition, it is important to understand the limited disclosure and publicity that they have brought to this issue in the public sphere. For example, Google's Public Policy blog has a post regarding their efforts on ECPA – but nowhere in the post or the accompanying video are the actual privacy considerations that users should take into account before using their products spelled out.[21] At the same time, Google advertises that one of the "top 10 reasons to use Gmail" is that it is "secure – just like bank websites."[22] Such claims divert attention from the serious privacy considerations that users should take into account when signing up to use such a service.

The motivations for such opacity are clear – many users would be alarmed by the lack of privacy in their electronic communications, and no company is anxious to lose its customers. However, from a public policy standpoint, this is alarming behavior. Therefore, in addition to supporting the efforts of the DDP coalition to update the ECPA statue, it is recommended that providers of cloud-based email services, as well as wireless carriers, make it clear to consumers exactly what their "reasonable expectation of privacy" means.

This can be done in a number of cost-effective ways – email providers, for example, could include a prominent disclaimer on email login splash pages. Wireless providers could prominently highlight this information among the myriad disclaimers that are included with any cellular phone. In addition to informing consumers about their expectation of privacy, these companies could advance their stated

---

[18] Office of Senator Patrick Leahy, *Leahy Introduces Benchmark Bill To Update Key Digital Privacy Law*, LEAHY.SENATE.GOV, **HTTP://LEAHY.SENATE.GOV/PRESS/PRESS_RELEASES/RELEASE/?ID=B6D1F687-F2F7-48A4-80BC-29E3C5F758F2**, (last visited Jan. 11, 2011).

[19] Senate Judiciary Committee Minority Counsel, *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age*, SCRIBD.COM, HTTP://WWW.SCRIBD.COM/DOC/38407733/REPUBLICAN-SENATE-MEMO-AGAINST-PRIVACY-AND-CLOUD-COMPUTING-REFORM, (last visited Jan. 11, 2011).

[20] Testimony of Associate Deputy Attorney General James Baker, *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age*, Hearing of the Senate Judiciary Committee, HTTP://WWW.GPO.GOV/FDSYS/PKG/CHRG-111SHRG66875/PDF/CHRG-111SHRG66875.PDF at 6, Sept 22, 2010.

[21] Richard Salgado, *An important step toward updating ECPA*, GOOGLEPUBLICPOLICY.BLOGSPOT.COM, HTTP://GOOGLEPUBLICPOLICY.BLOGSPOT.COM/2010/05/IMPORTANT-STEP-TOWARD-UPDATING-ECPA.HTML, (last visited Jan. 11, 2011).

[22] Google, *Top 10 reasons to use Gmail*, GOOGLE.COM, HTTP://MAIL.GOOGLE.COM/MAIL/HELP/INTL/EN/ABOUT.HTML, (last visited Jan. 11, 2011).

public policy and legislative goals – a population more educated about unexpected intrusions into privacy is more likely to demand reform to ECPA laws from their elected representatives.

Conclusion: Increased Transparency and Reform are Necessary

It is hopefully only a matter of time until revisions to ECPA that reflect the DDP principles are passed into law, and the operation of the law is brought in line to operate in concert with its laudable original goals. In the meantime, stakeholders should make a concerted effort to increase consumer awareness of existing privacy limitations.