Stanford Law Review Online

Volume 69 December 2016

ESSAY

Gotta Collect It All!: Surveillance Law Lessons of *Pokémon Go*

Brandon R. Teachout*

Days after the release of the mobile game *Pokémon Go*, a privacy flap ensued from press reports revealing that users on Apple phones who logged in through a Google account had unwittingly granted the developer, Niantic, access to their entire Google account. Moreover, the application's (app's) privacy policy allowed Niantic to disclose any information it possessed to third parties or the government for a range of purposes.[1] Niantic calmed the storm by stating that the permissions grant was not as sweeping as it appeared, that it had only accessed "basic Google profile information," and that it would update the app to request more limited permissions.[2] The privacy policy, however, remains unchanged.[3]

While this imbroglio highlighted that real-world societal expectations of privacy are significant, this Essay addresses something crucial that was not as widely discussed. The lack of clarity in three key areas of the legal regime covering electronic surveillance raises serious questions about the legal implications of everyday activities. Both Congress and the Supreme Court must act to ensure that the legal regime advances apace with new technology by updating the Stored Communications Act and recognizing a greater expectation of privacy with regard to information disclosed to third parties.

* J.D. Candidate, Stanford Law School, 2017.

1. *Pokémon GO Privacy Policy*, NIANTIC (July 1, 2016), https://www.nianticlabs.com/privacy/pokemongo/en.

2. *See* William Turton, *Pokémon Go Was Never Able to Read Your Email [Updated]*, GIZMODO (July 11, 2016, 7:28 PM), http://gizmodo.com/can-pokemon-go-really-read-all-your-emails-1783479136.

3. NIANTIC, *supra* note 1.

I. Legal Background

A. The Third-Party Doctrine

Per *Katz v. United States*, the seminal Supreme Court decision establishing the reasonable expectation of privacy doctrine, "the Fourth Amendment protects people, not places," but those things that "a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[4]

Thus, per *Smith v. Maryland*, information "voluntarily conveyed" to a phone company, and thereby exposed to the public, is not protected.[5] Specifically, the Court held in *Smith* that using a pen register to trace phone numbers dialed is not a search, even though recording "the *contents* of [a] conversation" would be.[6] *Smith* was grounded on two cases establishing that financial records voluntarily disclosed to a bank or an accountant were effectively exposed to the public if they were exposed to employees "in the ordinary course of business."[7]

In each of these cases, information was disclosed to a third party with the intention that that party would put it to use. A third party asked to complete a task must have access to the information required to do so, but not more: We expect the third party to carry a letter, not open it; to connect a call, not listen to it; to cash a check or file a tax return, not collect other unrelated content; and so on.

B. The Stored Communications Act

The Stored Communications Act (SCA), which governs disclosure of information to the government, similarly distinguishes content ("communications"), which enjoys the most protection, and other material ("records").[8] The SCA was enacted in 1986 as Title II of the Electronic Communications Privacy Act (ECPA) to update the 1968 Wiretap Act in order to resolve uncertainties created by then-new computer technology—in particular, "electronic mail."[9]

---

4. 389 U.S. 347, 351 (1967).

5. 442 U.S. 735, 744 (1979).

6. *Id.* at 742-43; *see also id.* at 744 (reasoning that electronic switching equipment "is merely the modern counterpart of the operator" who formerly heard the numbers while connecting calls).

7. United States v. Miller, 425 U.S. 435, 442 (1976) (banks); Couch v. United States, 409 U.S. 322, 335-36 (1973) (accountants).

8. *See* 18 U.S.C. § 2702 (2015) (voluntary disclosure); *id.* § 2703 (compelled disclosure). This Essay focuses on compelled disclosure.

9. S. REP. NO. 99-541, at 3-5 (1986) ("[T]he law must advance with the technology to ensure the continued vitality of the fourth amendment."); H.R. REP. NO. 99-647, at 18-19 (1986)

The SCA's definitions relate back to the Wiretap Act.[10] It defines the "contents" of a communication to include "any information concerning the substance, purport, or meaning of that communication."[11] In general, content is that which a user intends to communicate (for instance, the body and subject of an e-mail), and noncontent is information about the means by which it is communicated (for instance, usage logs and header information other than the subject).[12] Basic subscriber information is also a noncontent record.[13]

This line-drawing exercise is important because there are different privacy standards for content and noncontent. Content enjoys greater protection, with content in storage for 180 days or less requiring a search warrant for compelled disclosure and older content requiring a subpoena or court order and user notice.[14] Noncontent, by contrast, may be accessed through a subpoena or court order without notice.[15] The SCA applies to "the contents of any wire or electronic communication," as long as the communication is "held or maintained" by the provider "solely for the purpose of providing storage or computer processing services."[16] That means that e-mail and cloud data are protected, but content held by social networking sites or game developers may not be.[17]

The Supreme Court has not ruled on the constitutionality of the SCA,[18] but federal circuit courts have found warrantless collection of noncontent constitutional.[19] Only one circuit, the Sixth, has considered e-mail content, holding in *United States v. Warshak* that e-mails (like letters or phone calls) require a warrant to search, even if they are more than 180 days old.[20] The Sixth

("Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances.").

10. *See* 18 U.S.C. § 2711(1).

11. *Id.* § 2510(8).

12. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1228 (2004); *see also* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1019-20 (2010).

13. *See* 18 U.S.C. § 2703(c)(2).

14. *Id.* § 2703. The law allows voluntary disclosure only in particular cases, such as a dangerous emergency or if the provider inadvertently discovers child pornography or certain other evidence—or by consent of the user. *Id.* § 2702(b).

15. *Id.* § 2703(c).

16. *Id.* § 2703(b).

17. *See id.* § 2703(a)-(b); *see also, e.g.*, Declan McCullagh, *DOJ: We Don't Need Warrants for E-Mail, Facebook Chats*, CNET (May 8, 2013, 7:00 AM PDT), http://cnet.co/2fGOIC7.

18. Its only case even mentioning the SCA was *City of Ontario v. Quon*, 560 U.S. 746 (2010), which dealt with a government employee's expectation of privacy in a pager device supplied by an employer.

19. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001).

20. 631 F.3d 266, 286-88 (6th Cir. 2010).

Circuit distinguished "the mere *ability* of a third-party intermediary to access the contents of a communication" and "the *right* of access" from voluntary user disclosure.[21] It further distinguished e-mail providers (mere intermediaries) from the banks in *United States v. Miller* (third-party intended recipients directly involved in financial transactions).[22]

II. The *Pokémon Go* Kerfuffle

Pokémon Go is an "augmented reality" mobile game that uses smartphone features like cameras and location tracking to allow users to find and "catch" digital cartoons called Pokémon in the real world.[23] The game was a smash hit: within two days, it was installed on 5% of Android devices in the United States, and it rivaled Twitter for daily users.[24]

But a blog post two days after the game's release catalyzed privacy concerns: an engineer at a security analytics firm warned that the app was "a huge security risk," capable of accessing Gmail and Google Drive, Maps, and Photos.[25] Social media filled with posts warning about privacy problems, and tech blogs filled with alarmist headlines—updated to reflect a lower state of alarm[26] after more skeptical reporters dug into the technical details.[27] Niantic issued a statement saying that the permissions request was in error and only basic Google profile information had actually been accessed.[28] Soon thereafter, it released an updated version of the app.[29]

But serious privacy concerns remain. As the *Wall Street Journal* and even BuzzFeed noted, the app still tracks phone locations and IP addresses, and

21. *Id.* at 286-87.

22. *Id.* at 287-88 (distinguishing United States v. Miller, 425 U.S. 435, 442-43 (1976)).

23. Nick Wingfield & Mike Isaac, *Pokémon Go Brings Augmented Reality to a Mass Audience*, N.Y. TIMES (July 11, 2016), http://nyti.ms/29CGXJr.

24. Clara Ferreira-Marques, *Pokemon Game Adds $7.5 Billion to Nintendo Market Value in Two Days*, REUTERS (July 11, 2016, 10:44 PM EDT), http://reut.rs/29wIhiJ.

25. Adam Reeve, *Pokemon Go Is a Huge Security Risk*, TUMBLR (July 8, 2016), http://adamreeve.tumblr.com/post/147120922009/pokemon-go-is-a-huge-security-risk.

26. *See, e.g.*, Andrew Cunningham, *iOS Version of* Pokémon Go *Is a Possible Privacy Trainwreck [Updated]*, ARS TECHNICA (July 11, 2016, 7:00 PM), http://arstechnica.com/?post_type=post&p=921383 (revealing the original headline in the full URL: "Pokémon Go on iOS gets full access to your Google account").

27. *See, e.g.*, Turton, *supra* note 2 (reporting on Reeve's blog post, *supra* note 25, with information from other tech experts and Google itself).

28. *Id.*

29. *See* Brian Barrett, *Update Your* Pokémon Go *App Now to Fix That Privacy Mess*, WIRED (July 12, 2016, 3:08 PM), https://www.wired.com/2016/07/update-pokemon-go-app-now-fix-privacy-mess.

Niantic's privacy policy still allows extensive collection and sharing of data.[30] The policy allows disclosure of "any information" in Niantic's possession or control to the government, law enforcement, or private parties as it, in its "sole discretion," believes appropriate to respond to legal claims, protect property and people, and "stop any activity that [it] consider[s] illegal, unethical, or legally actionable activity."[31] These broader concerns led Senator Al Franken to write a letter to Niantic crediting it for fixing the Google account issue while expressing broader concern about the amount of data collected and the terms of the privacy policy.[32]

This outcry shows that the old saying "if you're not paying for the product, you are the product"[33] has resonated with the public. That people tolerate a loss of privacy to play *Pokémon Go* does not mean they like doing so.

III. The Gaps Revealed

In addition to the degree of general public unease about information privacy, this imbroglio highlights the shortcomings of current surveillance law in three key areas: the fuzziness of the content/noncontent divide, the overbroad nature of the third-party doctrine, and the potential for consumer privacy policies to incidentally authorize surveillance.

A. Content

Pokémon Go is a case study in how the content/noncontent distinction outlined in the SCA—and inherent in *Smith*—struggles in the face of twenty-first-century technology. The location information Niantic collects is almost surely noncontent, since it is the means by which the game digitally "places" Pokémon into the real world.[34] Similarly, the app requests permission to use a

30. Nathan Olivarez-Giles, *'Pokémon Go' Creator Closes Privacy Hole but Still Collects User Data*, WALL ST. J. (July 13, 2016, 9:11 AM ET), http://on.wsj.com/2acJv2t; Joseph Bernstein, *You Should Probably Check Your Pokémon Go Privacy Settings*, BUZZFEED, https://www.buzzfeed.com/josephbernstein/heres-all-the-data-pokemon-go-is-collecting-from-your-phone (last updated July 12, 2016) (noting the potential that law enforcement will access the data).

31. NIANTIC, *supra* note 1.

32. Letter from Sen. Al Franken to John Hanke, CEO, Niantic, Inc. (July 12, 2016), http://www.franken.senate.gov/files/letter/160712_PokemonGO.pdf.

33. *See* Derek Powazek, *I'm Not the Product, but I Play One on the Internet*, POWAZEK (Dec. 18, 2012), http://powazek.com/posts/3229 (criticizing the phrase).

34. Circuit courts have repeatedly held that information that can be used to triangulate a user's location, such as IP addresses or cell-site records, is noncontent unprotected by the Fourth Amendment. *See, e.g.*, United States v. Carpenter, 819 F.3d 880, 887 (6th Cir. 2016) (cell-site records); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (IP addresses).

phone's camera to "see" Pokémon atop real world surroundings.[35] These images are not sent to Niantic, but if they were, even they could be noncontent, part of the way Pokémon are "delivered." While *Pokémon Go* does not have in-game messaging, Niantic's first augmented reality game, Ingress, does. Those messages would definitely seem to be content—but, despite *Warshak*, it is still not clear that dynamic content like messaging is protected by the Fourth Amendment.[36]

B. Third-Party Doctrine

The Sixth Circuit in *Warshak* distinguished *Miller* in two ways: first, the bank documents at issue there were "simple business records," unlike "the potentially unlimited variety of 'confidential communications'" at issue in an e-mail account,[37] and second, the *Miller* bank documents were used "in the ordinary course of business," while the *Warshak* third party was an "*intermediary*, not the intended recipient of the emails."[38]

How would the data Niantic collects on *Pokémon Go* players fall into this scheme? It may depend. Suppose Niantic *had* accessed the e-mail accounts of certain users: it would not be an intermediary, let alone the e-mails' intended recipient. But the material was nonetheless disclosed. What if Niantic had accessed a user's tax return on Google Drive? The answer to each of these questions may depend on whether Niantic used the data "in the ordinary course of business," per *Smith*. But that may beg the question: if consumers are the product, *all* data collected are par for the course.

C. Privacy Policies

The third issue—perhaps the most important over the long term—is how privacy policies and other user consent agreements impact surveillance law. The court in *Warshak* noted that "the ability of a rogue mail handler to rip open a letter does not make it unreasonable to assume that sealed mail will remain private on its journey across the country."[39] Yet that property-based understanding does not translate precisely into the digital world. The SCA allows voluntary disclosure of content with user permission.[40] Accepting a

35. Jen McGuire, *How to Allow Camera Access on 'Pokemon Go' so You Feel Like You're in the Pokemon World*, ROMPER (July 20, 2016), https://www.romper.com/p/zhow-to-allow-camera-access-on-pokemon-go-so-you-feel-like-youre-in-the-pokemon-world-14708.

36. *See* McCullagh, *supra* note 17 (noting the Department of Justice's position that messaging is not content).

37. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (quoting United States v. Miller, 425 U.S. 435, 442 (1976)).

38. *Id.* (quoting *Miller*, 425 U.S. at 442).

39. *Id.* at 287.

40. *See supra* note 14.

privacy policy gives just this sort of permission. The Department of Justice itself pointed out that the privacy policies of many communications providers grant them far more access to user communications than rogue mail handlers.[41] So too the policies of developers like Niantic.

* * *

Summing up, the legal regime governing electronic surveillance lacks clarity in three key areas. First, the SCA's distinction between content and noncontent is too simplistic to handle hybrid data like messenger texts or aggregated metadata. Second, the *Smith* "course of business" standard is outdated when it comes to companies like Niantic, which require a significant amount of information just to provide their service, or Google, which is both an intermediary facilitating e-mail and an advertising company that scans e-mails to determine which ads to serve. And third, both the *Katz* reasonable expectation standard and the SCA's voluntary consent provision may be implicated by the overbroad contract-of-adhesion-style privacy policies that have become the norm.

IV. Once More into the Breach

What, then, is to be done?

The easy answer is that Congress should update the SCA to create additional privacy protections beyond those required by the Fourth Amendment.[42] In fact, it considered doing so earlier this year. In April, the House of Representatives passed the Email Privacy Act by a vote of 419 to 0.[43] That bill would codify *Warshak*, which the Department of Justice has voluntarily followed as a matter of national policy since 2013.[44] It would not refine the distinction between content and noncontent to resolve concerns about disclosure of messaging or other data, nor would it address aggregated metadata or other noncontent. And it would still allow disclosure of content "with the lawful consent of the

41. *Cf.* COMPUT. CRIME & INTELLECTUAL PROP. SECTION, DEP'T OF JUSTICE CRIMINAL DIV., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 146 (3d ed. 2009) ("Terms of service used by network service providers often establish that the provider has authority to access and disclose subscriber email.").

42. *See generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004) (arguing that Congress has traditionally acted to fill gaps between the privacy protections a reasonable person might want and those recognized under the Fourth Amendment).

43. *Final Vote Results for Roll Call 167*, U.S. HOUSE REPRESENTATIVES, http://clerk.house.gov/evs/2016/roll167.xml (last visited Dec. 15, 2016).

44. H.R. REP. NO. 114-528, at 9 (2016).

subscriber or customer,"[45] raising the question whether Niantic's privacy policy authorizing disclosure in its sole discretion amounts to such consent.

Despite these limitations, the bill enjoyed wide support from the public and tech sector as it moved to the Senate.[46] But it got bogged down in the Judiciary Committee thanks to a debate over whether the FBI should have the authority to compel disclosure of metadata via national security letter.[47] With the bill removed from the committee's markup calendar, it is dead for now. If Congress cannot even pass legislation that does little more than codify current policy, the odds of broader reform seem long. But the bill's overwhelming victory in the House, wide cosponsorship in the Senate, and broad support from the public and tech sector do suggest that the issue will remain on the legislature's radar. Nonetheless, the failure of the bill to resolve the broader issues raised above shows that even the action Congress is considering lags behind new technology.

Similarly, while the Supreme Court has yet to squarely address the issue of data privacy, there are signs that the Court, and particularly Justice Sotomayor, is thinking about it. In *Riley v. California*, the Court considered the "vast quantities of personal information" that cell phones contain in holding that police may not search a smartphone in a warrantless search incident to arrest.[48] And, concurring in *United States v. Jones*, Justice Sotomayor directly addressed the broad scope of the third-party doctrine, suggesting that warrantless disclosure of aggregated noncontent might violate the Fourth Amendment.[49] Indeed, five Justices in that case embraced the D.C. Circuit's mosaic theory, the idea that prolonged surveillance could, over time, constitute an unreasonable search.[50]

A future Supreme Court decision could read mosaic theory into the Fourth Amendment, resolving some concerns about apps like *Pokémon Go* that require extensive metadata to run. It could build on Justice Scalia's majority opinion in

45. Email Privacy Act, H.R. 699, 114th Cong. § 3 (2016).

46. *See Coalition Letter in Support of Email Privacy Act (April 26)*, CTR. FOR DEMOCRACY & TECH. (Apr. 25, 2016), https://cdt.org/?p=78320; *cf.* Andrea Peterson, *The Government Often Doesn't Need a Warrant to Get Your E-mails. But Most Think It Should.*, WASH. POST: THE SWITCH (Nov. 30, 2015), http://wapo.st/1NY0JaV (reporting that 77% of registered voters surveyed by Vox support a warrant requirement for compelled disclosure of online content).

47. *See* Alex Byers & Kate Tummarello, *Inside Hillary Clinton's Tech Policy Orbit*, POLITICO: MORNING TECH (May 27, 2016, 10:00 AM EDT), http://politi.co/1WQtWNX.

48. 134 S. Ct. 2473, 2485 (2014).

49. 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.").

50. *Id.*; *id.* at 964 (Alito, J., concurring); *see also generally* Gabriel R. Schlabach, Note, *Privacy in the Cloud: The Mosiac Theory and the Stored Communications Act*, 67 STAN. L. REV. 677 (2015) (explaining the mosaic theory and proposing an amendment to the SCA to incorporate it into statute).

Jones, repurposing his trespass doctrine to hold that data are property, regardless of where they are stored. It could conclude, as *Katz* did for phone calls, that the physical location of data is not crucial to determining societal expectations of privacy.[51] Or it could bring *Smith* into the twenty-first century by offering guidance on whether and how tech companies use data and metadata in the "ordinary course of business." While it is unclear what direction the Court will take, it is all but certain that creative new applications of technology like *Pokémon Go*—and the capacity of the government to exploit them—will require the Court to address the issue.

51. Data may in fact be relatively tangible. *See* Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 760-63 (2016).