Denver Law Review Forum

Volume 94 | Article 23

2-10-2017

An Initial Look at House Bill 17-1053—Warrant or Order for Electronic Communications

Joel Hamner

AN INITIAL LOOK AT HOUSE BILL 17-1053—WARRANT OR ORDER FOR ELECTRONIC COMMUNICATIONS

On January 11, 2017, the first regular session of the 71st Colorado General Assembly convened. Among the many bills proposed was House Bill 17-1053 (HB17-1053),[1] a bill for an act Concerning Orders For Electronic Communications. The bill—currently under consideration by the House Judiciary Committee—sets out to establish a warrant requirement for all government entities seeking electronic communication information from service providers.

In recent years, the issues of collective security, civil liberties, and the surveillance state have featured prominently in media headlines and pop culture references. Warrantless government access to electronic communications (and service providers' participation in affording that access) has received a significant share of attention in the ensuing dialogue. Even so, federal legislators have done remarkably little to address public concerns or resolve policy deficiencies. Consequently, the responsibility to initiate progress in this arena has fallen to the states—the "laboratories of democracy"—whereby state legislatures have the unappealing task of charting a legislative pathway between the demands of law enforcement and the protection of civil liberties in a complex and rapidly evolving technological environment. As unappealing as it may be, however, this is exactly the type of work a free and thinking society ought to expect of its government. Fortunately, HB17-1053 is an excellent step in the right direction toward accomplishing just such a task.

Before addressing the bill itself, a brief assessment of recent events and legal precedent on the subject will likely provide some beneficial context.

PART I—THE SOCIAL AND LEGAL CONTEXT FOR WARRANTLESS ELECTRONIC SEARCHES

In 2013, former-NSA contractor Edward Snowden disquieted millions with his revelation that the ultra-secretive spy agency was engaged in programs of mass electronic surveillance.[2] A number of these programs netted droves of wholly domestic communications in its digital trawling expeditions.[3] As disconcerted as many citizens felt by those

1. H.B. 17-1053, 71st Gen. Assemb., 1st Reg. Sess. (Colo. 2017).
2. *See* Paul Szoldra, *This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks*, BUSINESS INSIDER (Sep. 16, 2016, 8:00 AM), http://www.businessinsider.com/snowden-leaks-timeline-2016-9.
3. *See Id.*; *see also* [Case Title Redacted], 2011 WL No. 10945618, at *1 (FISA Ct. Oct. 3, 2011).

reports, further revelations generated an arguably greater ripple effect across the United States tech industry, as the documents alleged a creepily cozy relationship between the government's bevy of three-letter agencies and the people who provide the world with its email, social media, and phone services.[4] In total, nine leading technology companies were accused of complicity in the NSA's warrantless data collection program that collected emails, photographs, documents, video chats, connection logs, and more directly from electronic communication service providers.[5] Many customers felt outraged by the violation of trust—not merely by their government but (perhaps more poignantly) by their service providers.[6] As history will show, however, none of that should have come as a surprise.

In 1862, California became the first state to enact an anti-wiretapping law in an effort to protect the vital telegraph lines that connected western businessmen with their investors on the East Coast.[7] Following California's lead, New York and Illinois took steps in 1895 to safeguard their telephonic communication infrastructure with similar anti-wiretapping legislation.[8] By 1916, the courts were already embroiled in "America's first wiretapping controversy," as the New York Police Department had created a "wire tapping squad" that was found to have collaborated with local telephone companies to tap phone lines despite the above-referenced state law barring the practice (there was no exception for law enforcement, at the time).[9] In the years following, government entities doubled down on the new practice, rapidly expanding their reliance upon (and legal authorization for) warrantless electronic surveillance and collaboration with telephone service providers to the point that

---

4. *See* Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html; Nicole Arce, *Effect Of NSA Spying On US Tech Industry: $35 Billion? No. Way More*, TECHTIMES (June 10, 2015, 11:59 PM), http://www.techtimes.com/articles/59316/20150610/effect-of-nsa-spying-on-us-tech-industry-35-billion-no-way-more.htm; Laura K. Donohue, *High Technology, Consumer Privacy, and U.S. National Security*, 4 AM. U. BUS. L. REV. 11, 12–15 (2015).

5. Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, WASHINGTON POST, (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

6. Patrick Gray, *Tech Companies and Government May Soon Go to War Over Surveillance*, WIRED MAG., (Aug. 29, 2013, 9:30 AM), https://www.wired.com/2013/08/stop-clumping-tech-companies-in-with-government-in-the-surveillance-scandals-they-may-be-at-war/.

7. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 841 (2004).

8. *Id.*

9. Wesley MacNeil Oliver, *America's First Wiretapping Controversy in Context and As Context*, 34 HAMLINE L. REV. 205, 209 (2011); KERRY SEGRAVE, WIRETAPPING AND ELECTRONIC SURVEILLANCE IN AMERICA, 1862-1920, 129 (2014); Berger v. New York, 388 U.S. 41, 46 (1967).

"wiretaps [had become] the principal source of information" for police during the days of Prohibition.[10]

Even so, it was not until 1967 that the U.S. Supreme Court crafted a cogent method for analyzing the legality of warrantless searches of electronic communications. In *Katz v. United States*,[11] the Court held that warrantless searches are invalid where there exists a "reasonable expectation of privacy."[12] Moreover, that expectation of privacy is not tied to any structure, area, or geographic location; rather, the expectation of privacy follows the person that it protects.[13] In so holding, the Court ensured the fundamental safeguards of the Fourth Amendment's warrant requirement would protect citizens' electronic communications even at the dawn of the digital age. Or so it seemed.

Twelve years later, in *Smith v. Maryland*,[14] the Court held that government use of a pen register in a criminal investigation does not constitute a "search" as contemplated by the Fourth Amendment.[15] Its reasoning followed the logic that "in all probability [the accused] entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.'"[16] What is important for the purpose of this article is not so much the Court's flaccid analysis but the fact that the Court's decision legitimized extrajudicial collaboration between law enforcement and electronic communication service providers in criminal investigations.

In 1986, Congress passed the Stored Communications Act (SCA), codifying required disclosure provisions for electronic communication service providers, pursuant to a warrant based on probable cause.[17] Since that time, however, the courts have carved out a series of conditions under which the subject of investigation is not found to have a reasonable expectation to privacy—most notably, when the information sought is cell site location information, an Internet Protocol address, or subscriber information obtained via social networking and other service providers. But whether a person has a reasonable expectation to privacy regarding communications hosted by a third-party service provider has remained a contentious issue. The early years of the War on Terror provided an ideal

---

10. Thomas Y. Davies, *The Supreme Court Giveth and the Supreme Court Taketh Away: The Century of Fourth Amendment "Search and Seizure" Doctrine*, 100 J. CRIM. L. & CRIMINOLOGY 933, 937, 965–67 (2010); *Berger*, 388 U.S. at 46.

11. 389 U.S. 347 (1967).

12. *Id.* at 360 (J. Harlan, concurring). (In his concurrence, Justice Harlan laid out what has become the standard test of this reasonable expectation of privacy in a two-prong approach: first, "a person [must] have exhibited an actual (subjective) expectation of privacy and, second . . . the expectation [must] be one that society is prepared to recognize as 'reasonable.'") *Id.* at 361.

13. *Id.* at 351.

14. 442 U.S. 735 (1979).

15. *Id.* at 745–46.

16. *Id.* at 745.

17. 18 U.S.C. § 2703(a).

environment for the rapid expansion of government control in the digital domain. Notably, the 6th Circuit acknowledged in 2010 that a reasonable expectation to privacy existed in email communications, while also finding that a good faith reliance on the provisions of the SCA was all that was needed to compel disclosure of those same emails from a service provider.[18]

More recently, Apple, Inc. made headlines in the spring of 2016 for its dogged refusal to relinquish to the FBI the encrypted internal communications of one of the perpetrators of the mass shooting in San Bernardino, California.[19] The FBI obtained a court order instructing Apple to write new software with the purpose of breaking its own encryption.[20] In an open letter to the company's customers, Apple CEO, Tim Cook, stated his reason for defying the order was to "speak up in the face of what we see as an overreach by the U.S. government."[21] Some took the perspective that the authorities viewed the San Bernardino case as an ideal opportunity to advance the issue of mandating a government backdoor into private data encryption.[22] Despite the tense controversy, the legal showdown ended in a whimper when the FBI hired a secret third party to break into the phone and the entire issue faded from the public eye.[23]

PART 2—A LOOK AT THE CONSTRUCTION OF HB17-1053

The bill itself reads about as smoothly as a privacy policy statement accompanying a software update. Section 1 dives into a series of robust, technical definitions of terms such as "electronic communication information," "electronic communication service," and "subscriber information," with ample reference to the existing body of federal definitions.[24]

But the operative language of the bill is direct, stating: "A governmental entity may require a provider of an electronic communication service . . . to disclose the contents of an electronic . . . communication . . . *only* pursuant to a valid search warrant or court order for produc-

---

18. U.S. v. Warshak, 631 F.3d 266, 274 (2010).
19. Alina Selyukh, *A Year After San Bernardino And Apple-FBI, Where Are We On Encryption?*, NAT'L PUB. RADIO, (Dec. 3, 2016, 1:00 PM), http://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption.
20. *Id.*
21. Tim Cook, Apple CEO, *A Message to Our Customers*, APPLE, INC., (Feb. 16, 2016), http://www.apple.com/customer-letter/.
22. *See* Brian Barrett, *The Apple-FBI Fight Isn't About Privacy vs. Security. Don't' Be Misled*, WIRED MAG., (Feb. 24, 2016, 7:00 AM) https://www.wired.com/2016/02/apple-fbi-privacy-security/ (arguing that the whole fight over the phone's data was "a public relations maneuver," noting that the FBI had at least four other substantially similar legal disputes with Apple at the time but that the agency's focus on the San Bernardino case fit into a broader objective of securing "backdoor-friendly legislation from President Obama and Congress").
23. Selyukh, *supra* note 19.
24. H.B. 17-1053, 71st Gen. Assemb., 1st Reg. Sess. (Colo. 2017).

tion of records."[25] What follows from there is a thorough articulation of the (undeniably broad) scope of electronic communication information to which law enforcement may be entitled[26] followed by an expression of the probable cause standard[27] and a series of exceptions and exclusions that track with well-established law related to police search and seizure practices.[28] The bill contains a notice provision for the target of the investigation; an exclusionary rule; and both standing and release-of-liability provisions, by which service providers may either challenge or comply with the terms of a warrant.[29] The bill ends with a brief section highlighting service providers' federal right of voluntary disclosure of electronic communication at any time.[30]

PART 3—THE IMPORTANCE, IMPACTS, AND IMPLICATIONS

This bill has been a two-year project for its lone sponsor, Representative Lois Landgraf. In that time, Rep. Landgraf has done an excellent job of coalition building in order to, in her words, "get it right."[31] She brought law enforcement entities, district attorneys, business leaders, and civil liberty NGOs to the same table to hash out the nuts and bolts of what she hopes is an equitable solution to a highly controversial issue.[32] The result is a remarkably unremarkable bill full of exhaustively defined terms and a healthy list of exceptions. The real significance of HB17-1053 is under the hood. Specifically, the significance is found in the fact that the bill removes the question of the reasonableness from the courts as related to governmental search and seizure of citizens' electronic communications.

Like the Fourth Amendment to the U.S. Constitution, Article II, Section Seven of the Colorado Constitution erects a "reasonable" standard for warrantless searches and seizures. And while warrantless searches have historically been viewed as "presumptively invalid" under both constitutions,[33] the Colorado Supreme Court has also made clear that "[i]n the absence of a reasonable expectation of privacy, law enforcement officials are free to conduct a warrantless search."[34] But, by stating that government entities may obtain citizens' electronic communication information from service providers *only* upon presentation of a warrant, subpoena, or court order, HB17-1053 preempts the judicial inquiry into

---

25. *Id.* § (2)(a) (emphasis added).
26. *Id.* §§ (2)(a)(I)–(III).
27. *Id.* § (2)(b).
28. *Id.* §§ (3)–(5).
29. *Id.* §§ (6), (7), (9)–(11).
30. *Id.* § (12).
31. Rep. Lois Landgraf, Remarks at Stakeholders Meeting for HB17-1053 (Jan. 24, 2016).
32. *Id.* The author was present for this stakeholders meeting and noted the affiliations of the individuals in attendance.
33. People v. Berdahl, 2012 COA 179, ¶ 16.
34. People v. Salaz, 953 P.2d 1275, 1277 (Colo. 1998).

whether a reasonable expectation of privacy exists at all.[35] Rather than obliging to the creation of public policy by judicial precedent, HB17-1053 endeavors to enact it. This is an appropriate exercise of legislative authority.

A 2016 report by the Pew Research Center found that American public opinion regarding privacy and security concerns has vacillated over the past decade—rising and falling with changing headlines and emergent world events.[36] How ought courts balance these ever-shifting anxieties? How do judges craft an objective standard of reasonableness from that? In reality, the legislature is the branch closest to the people. Thus, the legislature is the branch best suited to embrace these questions and set forth policy. This is precisely the goal of HB17-1053. While certainly not the final step in establishing a coherent and sensible policy for electronic search and seizure, this bill provides an excellent first step in the right direction.

Joel L. Hamner[*]

---

35. Interestingly, HB17-1053 lists "subscriber information" as a form of "electronic communication information." H.B. 17-1053 § (1)(b), 71st Gen. Assemb., 1st Reg. Sess. (Colo. 2017). In so doing, HB17-1053 signals a departure from a growing body of federal jurisprudence that finds no expectation of privacy in this information.

36. Lee Rainie & Shiva Maniam, *Americans feel the tensions between privacy and security concerns*, PEW RES. CTR., (Feb. 19, 2016), http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/.

* Joel Hamner graduated from the United States Naval Academy (with Honors) in 2009 and served for five years as an active duty Information Warfare Officer in the U.S. Navy. He entered the University of Denver Sturm College of Law in May 2014 and will graduate in December 2017. This article draws in part upon the final stakeholders meeting hosted by Rep. Lois Landgraf on January 24, 2017, just prior to discussion of the bill by the Colorado House Judiciary Committee.