Does the 4th Amendment offer effective privacy protection in a digital environment?

Dakoda Koziol

College of Southern Idaho

Does the 4th Amendment offer effective privacy protection in a digital environment? An important aspect of the tyranny of the British government was the liberties they took to search for and/or seize property for their purposes, including proving dissent. When the Bill of Rights was passed, the 4th Amendment guaranteed the right to privacy to U.S. citizens. Privacy is a vital pillar of the United States' democracy. Yet, although the 4th Amendment typically provides adequate protection of physical properties, it has unfortunately been poorly interpreted and administered for data properties, particularly digital communications. Between the actual text of the 4th Amendment, it's interpretations and administrations, and potential paths forward we can understand what went wrong with digital privacy and how to fix it.

What exactly does the 4th Amendment mean?

A transcript of the 4th Amendment in full:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." (U.S. Const., Amend. IV)

The Founders made it clear that when it is necessary to search a property, it should only be as extensive as required to solve a case. The phrase "probable cause" prevents a warrant from being granted without evidence of a crime. The phrase "particularly describe the thing to be seized" ensures that the warrant doesn't tread on the searched person's privacy anymore than it has to.

Jim Harper, digital privacy advocate, outlined how courts should apply the 4th Amendment: "Was there a search? Was there a seizure? Was any search or seizure of 'persons, houses, papers, [or] effects'? Was any such search or seizure reasonable?" He states that the words 'search' and 'seizure' are defined in the most basic ways that they can: a search is

"focused sensing that is often signaled by efforts to bring exposure to concealed things", and a seizure is the "government invasions of any property right". By knowing the basic definitions of search and seizure, and by finding parallels between the secured properties listed to modern properties, Harper argues that the 4th Amendment can be tightly and consistently administered in all cases of government invasion of privacy. (Harper)

How is the 4th Amendment interpreted to applied to digital environments?

The 4th Amendment typically protects the privacy of a person's physical properties, but modern communications are often exposed to government searches. A number of court decisions over the years have misplaced and ignored digital property rights and diluted the 4th Amendment for many data properties, especially digital.

In *Olmstead* (1928), a wiretapping case, Justice Butler had a notably direct interpretation of the case. In fact, Jim Harper credits him for the method outlined earlier.

> "The contracts between telephone companies and users contemplate the private use of the facilities employed in the service. The communications belong to the parties between whom they pass. During their transmission, the exclusive use of the wire belongs to the persons served by it. Wiretapping involves interference with the wire while being used. Tapping the wires and listening in by the officers literally constituted a search for evidence." (Harper)

By identifying property rights, the existence of a search of the property, and insinuating the existence of seizure of the exclusivity of those property rights, he ticked every point. In addition, if "probable cause" of a crime existed, a warrant would have been issued. Since this wasn't an emergency situation the search was "unreasonable". The 4th Amendment was clearly breached.

Unfortunately, that statement was Justice Butler's dissent. The court found that the 4th Amendment was not breeched.

Katz v. United States (1967) decided that the 4th Amendment only applies when "a person have exhibited an actual expectation of privacy" and "the expectation be one that society is prepared to recognize as 'reasonable.'" This logic is vague and subjective, and added a pointless buffer between the 4th Amendment and U.S. Citizens. Any property that requires a search to be exposed is inherently private and not in plain sight, regardless of whether a judge believes that the person searched expected privacy, or what a judge believes about what society believes is "reasonable". This way of interpreting the 4th Amendment also paved the way for third party doctrine: the idea that when property (especially data and communications) is entrusted to a third party, the "expectation of privacy" no longer exists. This creates a grey area for data properties owned by an individual but hosted by a third parties. (Harper) (Stanley, 2017)

Outside of court precedent, the Electronic Communications Privacy Act (ECPA, 1986) lets the government use a warrant to retrieve a person's communications from the service hosting them, instead of the person communicating, who owns those communications. It applies to email, cloud storage, and any data hosted online. For legal context, to search an apartment, the landlord's permission doesn't typically waive the need for a warrant. This is because the apartment is in effect the renter's property, allocated to the renter by their landlord. Parallels can be drawn to a cloud service allocating space on their servers to the individual who owns the data stored on them, and many other third-party services (Schwartzbach, 2017) (Cunningham, 2016)

Warrants for the search of online data rarely outline what should be searched "particularly". Clark D. Cunningham claims that more often than not warrants for digital communications require whole email accounts – everything from their creation to present day –

to be sifted through. Additionally, warrants of this type are often sealed. The government doesn't have to disclose the search, and the data host is put under a gag order, so person will never know that they were searched or part of a search unless they're tried based on evidence from that search. But perhaps the most blatantly outdated (or plain wrong) part of the ECPA is the 180-day rule, where online data more than 180 days old is considered abandoned and doesn't require a warrant to be searched. This is clearly ridiculous in the time of email and cloud storage. A file stored on Microsoft OneDrive is (or should be) a person's property from the moment it was stored to the day they relinquish it. When the government accesses those files without the persons permission, that is a "seizure" of the persons exclusive access to those files. Reading them is a "search". By the 4th Amendment, a warrant granted with "probable cause" is required. (Schwartzbach, 2017) (Cunningham, 2016) (Greenberg, 2017)

Executive Order 12333 (1981) grants the NSA permission to collect and search any foreign communications. The order was *somewhat* reasonable in the days before the World Wide Web, invented in 1989, but modern communications can run through any number of servers around the world, even when both the sender and recipient are stateside. This data, because it ran through a foreign server, is free game to the NSA. Searches of foreign data don't require a warrant or oversight, and so when foreign and international companies provide online services to American customers, they are inherently not private, not to the U.S. Government. (Greene, 2017)

Steps forward

The government should only be able to get a warrant to search an individual's communications, not the company providing those communications. When that individual doesn't comply with the search, and it's warranted, then the government can go to the company. In either case, only the data relevant to the case should be searched for, or at the very most kept.

Conducting a search on any person's property, including their communications data, should always require a warrant with probable cause regardless if that data is hosted by a third party or not. Notably, Utah recently passed a bill guaranteeing just that, taking the lead in the national movement to fix digital privacy. The bill was passed on the twelfth of March 2019. (Davis, 2019)

Foreign searches that will certainly involve American peoples' data (e.g. searches of international corporations known to have customers in the U.S.) should require a warrant and only keep data relevant to the case. If a customer's data is being searched unwarranted, and if the customer is an American citizen, then the 4th Amendment has been compromised, whether the search happened on American soil or not.

Finally, a person being searched should be notified when they have been searched, including broad searches such as foreign communications and third-party communications as described above. Obviously, exceptions to this rule should be granted for what the court decides are particularly sensitive cases, but they should be just that – exceptions to the rule.

In conclusion

It is clear in hindsight that the U.S. Government hasn't been perfectly faithful to the 4th Amendment. It has struggled to recognize new types of property at almost every technological advancement and is still struggling to protect digital properties today – but it shouldn't be. The 4th Amendment doesn't need to be interpreted. Its language is concise, clear, and basically defined to be near future-proof. Property is private by default, and for the government to access it requires a scope-limited warrant issued with probable cause. The only variable that time can change is the types of property. Moving forward, more careful analysis 4th Amendment should be practiced. If it was understood more literally, new digital privacy laws wouldn't even be needed.

References

Cunningham, C. D. (2017). Feds: We can read all your email, and you'll never know. In Betsy Maury (Ed.), *The Reference Shelf: Internet Abuses and Privacy Rights* (pp. 186-189). Ipswich, MA: H.W. Wilson. (Original work published 2016)

Davis, M. (2019, March 22). Utah Just Became a Leader in Digital Privacy. Retrieved March 22, 2019, from https://www.wired.com/story/utah-digital-privacy-legislation/

Green, R. (2017). Now it's much easier for government agencies to get NSA surveillance data. In Betsy Maury (Ed.), *The Reference Shelf: Internet Abuses and Privacy Rights* (pp. 63-65). Ipswich, MA: H.W. Wilson. (Original work published 2017)

Harper, J. (n.d.). National Constitution Center. Retrieved March 23, 2019, from https://constitutioncenter.org/digital-privacy/The-Fourth-Amendment-in-the-Digital-Age

Greenberg, A. (2017). Passing the email privacy act has never been more urgent. In Betsy Maury (Ed.), *The Reference Shelf: Internet Abuses and Privacy Rights* (pp. 13-15). Ipswich, MA: H.W. Wilson. (Original work published 2017)

Schwartzbach, M. (2017, September 15). Can Your Landlord Allow the Police to Search Your Apartment? Retrieved March 22, 2019, from https://www.nolo.com/legal-encyclopedia/can-your-landlord-allow-the-police-to-search-your-apartment.html

Stanley, J. (2016). The privacy threat from always-on microphones like the Amazon Echo. In Betsy Maury (Ed.), *The Reference Shelf: Internet Abuses and Privacy Rights* (pp. 77-82). Ipswich, MA: H.W. Wilson. (Original work published 2017)

U.S. Constitution, Amendment IV