Privacy and The Internet of Things: Perspectives on Mass Surveillance in the United States

Nishant Jain
CPSC 610
4/25/18

Broad Theme to Consider

Modern Trade-off: Privacy vs Security

Does the government have the right to collect sensitive information on all of its citizens if it means keeping the country safe?

Should we give up our constitutionally-granted right to privacy for security?

There are arguments on both sides of this debate...

Fundamental Questions: Looking Forward

The advent of the Internet of Things will provide vast new opportunities for mass surveillance

-How do fourth amendment protections factor into the ability of government agencies to use IoT devices for surveillance?

-Are U.S. citizens constitutionally protected from mass surveillance in the new digital age?

Outline

I. About the NSA, current programs, and mass surveillance
II. Introduction to the Internet of Things (IoT)
III. Discussion of Fourth Amendment protections as they apply to IoT-mediated surveillance
IV. Discussion of Third-Party Doctrine as it relates to accessing personal digital data

Historical Context

Post 9/11, there was a reaction by lawmakers to combat domestic terrorism

Can be argued that 9/11 was the catalyst that transformed U.S. into modern surveillance state

The NSA implemented mass surveillance programs

What is mission of the NSA?

Stands for National Security Agency

“Through carrying out its missions, NSA/CSS helps save lives, defend vital networks, and advance our Nation's goals and alliances, while strictly protecting privacy rights guaranteed by the U.S. Constitution and laws.” - NSA website

Two missions:

1) **Signals Intelligence (SIGINT) -** “gather information that **America's adversaries** wish to keep secret”
2) **Information Assurance** - “preventing unauthorized access to sensitive or classified national security information and systems” - NSA website

Signals Intelligence (SIGINT)

Definition: “Collecting foreign intelligence from communications and information systems and providing it to customers across the U.S. Government, such as senior civilian and military officials”

Purpose: “the information [is then used] to help protect our troops, support our allies, fight terrorism, combat international crime and narcotics, support diplomatic negotiations, and advance many other important national objectives.”

Emphasis on “foreign intelligence”

Shift to Domestic Mass Surveillance

Historically, the NSA focused on foreign surveillance. This changed dramatically in the 21st century.

There are many ways that the NSA is collecting your data without your knowledge.

Why?

To deem whether you are a national security threat and to gather intelligence in the fight against terrorism.

What is New? The Scale.

The scale of sensitive personal information that can be monitored by government agencies has increased.

Some things that the NSA monitors:

Internet history, Search History, Emails, Skype Calls, Phone Call History, Instant Messaging, Social Media Posts/Profiles, and more.

In the age of IoT, potential for even more data collection.

List of Several NSA Programs

1. **President's Surveillance Program:** For domestic surveillance of data traffic
    a. Two components: Bulk Communications Collection and Phone Metadata Collection
2. **PRISM:** Program to get user data directly from technology companies
3. **Program to check movement/association/location habits.**
4. **Five Eyes:** International coalition of intelligence sharing organizations

Bulk Collection: the strategy is to collect as much information as possible about everybody to detect potential threats and associations between enemy actors. Consider if this conflicts with the spirit of the 4th amendment.

The Internet of Things (IoT)

-Everyday objects that have embedded computing systems that allow them to connect to the internet. Can interact with the physical world to perform actions or generate insights.

-Restrict definition to only include devices that can collect, store, and transmit information from the physical environment around them.

-Ex: GPS sensors, Smart Thermostats, voice-based AI assistants, Heart-rate/fitness monitors

IoT Proliferation

Many companies working in this space. (Google, Nest, Amazon, Apple, Fitbit, etc)

Gartner predicts there will be 25 billion IoT devices in the world by 2020.

Ex:

-Smart Assistants: Google Home / Amazon Alexa

-Nest Cameras

-Apple Smartwatches / Fitbit Health Monitors

IoT as Surveillance:

Many IoT apps are implicitly built for surveillance: gather data about your habits and learn patterns.

> Ex: Consider fitness tracking apps that learn your morning run routine or smart home apps that learn your occupancy habits for turning on/off lights

Data that can be collected: location, voice, visual, audio, medical, tactile, etc.

Can provide detailed view of habits, health, and lifestyles of individuals.

Basically, IoT offers a trove of data for surveillance. But what about conflicts with the fourth amendment? Privacy concerns?

The Fourth Amendment

Transition to discussing privacy law as it relates to IoT-based surveillance.

"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."

What is an effect? Personal Property? Is it the device or the data? Or both?

Evolving Definitions

The definitions of each of these terms (person, house, papers, and effects) have been expanded over time.

Ex: House now means the home and the curtilage (surrounding parcel of land)

Ex: Person now has expanded to mean corporations as well as pockets on one's "person" in this 4th amendment context.

Precedent for changing of meaning as time goes on. Can be applied to effects as well when considering questions about the nature of digital data.

Effects in the Digital Age

In an article published in the California Law Review, Ferguson argues that effects can refer to both the physical device and the digital data stored on a device.

Riley v. California (2014): Searching the digital data contents (call-log, pictures, etc) of a cell phone in an arrest situation required a warrant.

Implications:

-Draws distinction between physical object and digital data

-Requires a warrant for government agents to search digital contents of a device

-Similar Argument can be applied to afford fourth amendment protections to searches of IoT devices

Devices in the Home

Ferguson provides even more support for fourth amendment protections on information originating from IoT devices in the home.

Kyllo v. United States (2001): Supreme Court ruled that the use of thermal sensor equipment by law enforcement officials to detect heat conditions within the home of a suspected marijuana-producer constituted a "search"

-Provides a precedent for requiring government agencies to acquire a warrant to gather information about conditions within one's home

Devices in the Home

Florida v. Jardines (2013): Supreme Court ruled that the capture by a trained dog of the smell of marijuana originating from a home constituted a "search"

Implications:

-Not merely temperature information, but also other broader conditions within a home such as smells, are protected under the fourth amendment

-Information originating from within the curtilage of the home is afforded fourth amendment protections. Ferguson argues that this can be interpreted to include signals that are transmitted from IoT devices within the home

Devices on One's Person

Examples:

-Body cameras such as Go-Pro cameras

-fitness devices such as

Fitbit sensors which can collect data on heart rates, location, and movement

Riley v. California (2014):

-Offers a precedent for the handling of IoT devices that may be present on one's person, since it was ruled that searching the digital data contents of a device found on one's person required a warrant

Summary of Fourth Amendment Protections

Appears to be legal precedent to invoke fourth amendment rights in the context of government agencies searching digital data gathered by IoT devices in both the home and on one's person

-Fourth amendment is therefore a valid defense against mass surveillance data collection implemented upon directly upon IoT devices

-Though these cases deal primarily with traditional law enforcement, the need for a warrant can apply to searches conducted by other government agencies including those such as the NSA that run mass surveillance programs

The Third-Party Doctrine

Third-Party Doctrine: American citizens cannot claim fourth amendment protections upon information voluntarily shared with third parties, as long as the government agencies acquire this information from the third party

Smith v. Maryland (1979): ruled that obtaining one's information voluntarily given to a third-party, such as a bank or phone company, would not constitute a search under fourth amendment definitions

-Third-party doctrine has been used to argue that NSA bulk collection programs for phone meta-data are consistent with the fourth amendment

-PRISM program also side-steps fourth amendment protections by obtaining user data directly from technology companies such as Google, Apple, and Facebook

Third-Party Doctrine and the Digital Age

-Critics of the third-party doctrine contend that it is outdated when it comes to the issues of personal digital data and communications

-Scale and invasiveness of electronic data was not anticipated at the formulation of the doctrine in the 1970's

"Voluntarily" Giving Up Information

Most IoT device manufacturers require users to share their data with them as part of lengthy user agreements.

Furthermore, most users do not even read these agreements because of the convoluted languages used to structure them.

As a result, many people are not even aware that they are signing away their privacy by using these devices or that they are allowing third parties access to this data.

It can therefore be argued that this data is not being "voluntarily" given to third-parties, and therefore may not be subject to search without a warrant by governmental agencies under the third-party doctrine

Revisiting Third-Party Doctrine in the Context of IoT

Given the invasive nature of data gathered by IoT devices that can be present both in one's home and on one's person, it can also be argued that there is a reasonable expectation of privacy with regard to the operation of these devices

Katz v. United States (1967): The legal test of reasonable expectation of privacy is the standard by which the applicability of fourth amendment protections is determined

Third-party doctrine as applied to gathering all digital personal data captured by IoT devices and originating from the home and one's person, seems to betray the spirit of fourth amendment protections from warrantless search

Revisiting Third-Party Doctrine in the Context of IoT

May suggest a need to revisit the legality of the third-party doctrine as it applies to digital personal data.

Jones v. United States (2014): opinion shared by Justice Sotomayor that the application of the third-party doctrine is "ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks"

Till this question is addressed by the courts, however, it appears that intelligence agencies will be legally allowed to use the Internet of Things to monitor the U.S. populace on a scale yet unimagined.

References

[1] W. Post, "Nsa slides explain the prism data-collection program," *Washington Post*, 2013. Accessed: 2018-04-24 at `http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/`.

[2] "About nsa." `https://www.nsa.gov/about/faqs/about-nsa-faqs.shtml`, May 2016. Accessed: 2018-04-24.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[4] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[5] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[6] "Predicts 2015: The internet of things," *Gartner*, December 2014. Accessed: 2017-05-03 at `http://www.gartner.com/newsroom/id/2970017`.

[7] "Constitution of the united states," 1787.

[8] A. G. Ferguson, "The internet of things and the fourth amendment of effects," *Cal. L. Rev.*, vol. 104, p. 805, 2016.

References

[9] M. E. Brady, "The lost effects of the fourth amendment: Giving personal property due protection," *Yale LJ*, vol. 125, p. 946, 2015.

[10] *Riley v. California.* Supreme Court of the United States, 2014.

[11] *Kyllo v. United States.* Supreme Court of the United States, 2001.

[12] *Florida v. Jardines.* Supreme Court of the United States, 2013.

[13] R. M. Thompson, *The fourth amendment third-party doctrine.* Congressional Research Service, 2014.

[14] *Smith v. Maryland.* Supreme Court of the United States, 1979.

[15] O. S. Kerr, "The case for the third-party doctrine," *Mich. L. Rev.*, vol. 107, p. 561, 2008.

[16] E. Murphy, "The case against the case for third-party doctrine: A response to epstein and kerr," *Berkeley Tech. LJ*, vol. 24, p. 1239, 2009.

[17] J. D. Mornin, "Nsa metadata collection and the fourth amendment," *Berkeley Tech. LJ*, vol. 29, p. 985, 2014.

References

[18] *Katz v. United States.* Supreme Court of the United States, 1967.

[19] *United States v. Jones.* Supreme Court of the United States, 2012.

[20] J. Rosen, "A liberal-conservative alliance on the supreme court against digital surveillance," *The Atlantic*, 2017. Accessed: 2018-04-24 at `https://www.theatlantic.com/politics/archive/2017/11/bipartisanship-supreme-court/547124/`.