Pirates of Privacy: How Companies Profit Off Your Personal Data by Using Capital Surveillance Methods in Criminal Prosecution

Shayna Koczur
Brooklyn Law School, New York City, NY*
https://doi.org/10.38126/JSPG210106
Corresponding author: shaynakoczur@gmail.com
Keywords: privacy; constitutional law; capital surveillance; law enforcement
*Author wrote article while with this affiliation

Executive Summary: Surveillance involves monitoring an individual as a method of obtaining information for future use, and is defined as continuous observation of a place, person, group, or ongoing activity in order to gather information. Governments are normally restricted by judicial safeguards such as warrants and common law when it comes to surveillance methods of obtaining an individual's private data. However, private companies are not. When users agree to terms and conditions on technology apps they often are not aware that they are consenting to being monitored and their information could easily be sold, even to the government. This process of capturing and commodifying personal data for profit-making is commonly referred to as "surveillance capitalism". Surveillance capitalism poses a threat to privacy rights because the methods by which users' online data is collected are overly intrusive due to the nature of how the data is stored on these apps. Additionally, the data collected by private companies can be sold, distributed, and used against the user's legal interests and liberties. However, both International Law and the United States Constitutional Law recognize the right to privacy. This raises the question: How do we protect privacy rights when much of our personal data is now stored digitally and on technological applications that society is becoming reliant on for everyday tasks? Privacy laws have not yet adapted to address this modern day challenge. This article discusses the legal understanding of privacy rights, the threat modern-day surveillance capitalism poses to those rights, and possible solutions for updating outdated privacy laws.

I. The legal concept of privacy rights

The United States Constitution states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated". The International Declaration of Human Rights states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks" (United Nations, 1948). Based on these doctrines, many sovereign nations recognize when collecting evidence in a criminal case that those accused of a crime have a reasonable amount of privilege to private information during an investigation. As crime and criminal law change and adapt to modern technology, the convenience of surveillance capitalism, the commodification of personal data for profit making, can be tempting as an effective way to gather evidence. However, when used by governments, surveillance capitalism is uncharted territory that could substantially violate privacy rights.

The use of surveillance capitalism provides the ability to gather evidence that has typically never before been used without a warrant in criminal prosecution (Kennedy, 2020). For example, a California man was charged with the murder of his step-daughter after her Fitbit revealed that the woman's heart rate significantly spiked, then ceased during the same timeframe as a neighbor's security camera showed the man's car was parked in her driveway (Hauser, 2018). Prosecutors used these

two modes of surveillance to prosecute him for murder.

Unlike in the physical world, where there are clear boundaries defining what is considered private data, there is no universally agreed-upon understanding of when personal data stored in the online world is protected by privacy rights. Though not International Law, the United States' criminal procedure case law can give guidance on how surveillance is a unique form of data collection that exceeds traditional privacy rights. In the United States' criminal law, the Third Party Doctrine states that people forfeit their privacy rights when they willingly divulge information to another person or entity (Koch, 2022). Examples of this include going to the bank and withdrawing money or understanding that your cell phone company knows who you call. However, providing information to a bank or cell phone provider is a minimal privacy intrusion compared to long-term general surveillance. The Third Party Doctrine does not, however, legalize the long-term surveillance of data which users do not know is being stored.

United States case law notes that extensive long-term surveillance encroaches on privacy interests and is more than merely providing information due to the nature of its invasiveness. For example, in United States v. Jones (2012), the Supreme Court held that attaching a Global Positioning System (GPS) to an individual's motor vehicle for the purpose of surveillance violates the defendant's privacy rights on the grounds that the GPS is a "trespass on the defendant's personal effects". In this case, officers had a valid warrant to attach a GPS mechanism on the defendant's car for several days. Law enforcement attempted to admit evidence into Court from the GPS that was attached to the defendant's car from subsequent days that were not authorized in the original warrant. The defendant argued that his privacy was invaded, and that an unlawful government search had occurred. He won his case because the Supreme Court defended the defendant's reasonable expectation of privacy and held the Fourth Amendment, which "extends to a person's freedom from unreasonable search and seizure beyond merely their person, but also as to their houses, papers, and effects" (Legal Information Institute).

Put simply, if someone reasonably believes that what they are doing is private, then their conduct is protected from surveillance and a warrantless search. In this case, law enforcement could not use GPS technology without a warrant to surveil the defendant's constant movement in his car. Though law enforcement argued that the defendant did not have a privacy interest in his movement because he was in public, the Supreme Court expressly said that even the Third Party Doctrine needs to be reconsidered due to digital data being so pervasive. Justice Alito said, "This approach 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. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their internet service providers; and the books, groceries, and medications they purchase to online retailers." He suggests that if users share data with an app or third party with a limited purpose of carrying out a mundane task, then they have a reasonable expectation of privacy in that data.

Further, in United States v. Carpenter (2018), the Supreme Court held that tracking a defendant's location via his cell phone as evidence was "too permeating" of a forum of surveillance and violates the defendant's privacy rights. The Supreme Court stated, "With access to cell phone location tracking, the government can now travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers, which currently maintain records for up to five years". The Court found this practice unconstitutional because of the voluminous amount of information that can be gathered from cell phone towers. The Court stressed that cell phone data can reflect when we go to the doctor or even when we engage in political activity, and this information is the result of exhaustive surveillance that should not be obtained without a warrant. In this case, law enforcement attempted to use several months of cell phone data without requesting a warrant.

These cases imply that though data may be offered and available by users to third parties, there is a crucial difference in government accessing data that was willfully offered by the defendant to a third, private party, and government requesting or

purchasing data from a private company that was obtained by ongoing invasive and permeating surveillance. Therefore, the U.S. government should not be allowed to access data that is obtained through surveillance capitalism without a judicial safeguard such as a warrant. Furthermore, if tracking someone's constant location via GPS or their cell phone is considered "too permeating", monitoring their search history, health records, and digital online activity is as well.

II. Use of surveillance capitalism by government actors in the U.S. and traditional privacy rights

Surveillance capitalism involves collecting data for profit, primarily for the benefit of private companies. Consumers often blindly consent to data collection policies through signing terms agreement provisions when they join social media platforms, such as Facebook, or even when they purchase an airline flight. This gives private corporations access to a wide variety of users' data. However, users usually do not realize that they agreed to have their information monitored, then possibly sold. In the physical world, the U.S. government cannot search one's effects if they have a reasonable and foreseeable expectation of privacy in their data. Furthermore, users do not reasonably expect their data to be used in criminal prosecution. A recent study showed that 49% of Americans answered that it is unacceptable for smart speaker companies to share audio recordings of their customers with law enforcement in order to help with criminal investigations, while only 25% said it is acceptable (Auxier, 2019).

What is uniquely problematic is when law enforcement can buy information that private companies gained through surveillance. In most cases, a warrant serves as a judicial safeguard to ensure this does not happen and technology companies usually have to comply with warrants. However, a warrant requires probable cause in order to "search" or "seize" the data that is desired (Legal Information Institute). Therefore, law enforcement needs to, in good faith, believe that the defendant has committed an offense. But, what happens before there is probable cause to issue a warrant? What happens when the government can buy a software program that has the fruits of a private company engaging in constant surveillance and uses it without a warrant?

For example, a *New York Times* investigation revealed that, in the past year alone, over 600 law enforcement agencies in the U.S. and Canada registered to use software from technology startup Clearview AI that can match uploaded photos against over three billion images scraped from the internet, including Facebook and YouTube (Fingas, 2021). Contracts to use the service cost as much as US$50,000 for a two-year deal. Often, this service is used to locate defendants.

This is problematic because by purchasing this software, the government can pay private companies to surveil individuals for them, then claim that they obtained the material from a third party which obtained the user's consent. Practices like these are problematic because even if the user did consent by signing the terms and agreements, users do not reasonably expect capital surveillance to engage in practices that are illegal, invasive, and unethical in the physical world.

The Wall Street Journal reported that the Department of Homeland Security's Customs and Border Protection (CBP) and Immigrations and Customs Enforcement (ICE) used location data from Venntel, a data analytics company, to locate undocumented immigrants and the routes they used to cross the border. Records show that CBP has given Venntel hundreds of thousands of dollars to access its location database. Considering the law in light of this practice, it can be deduced that government agencies are buying data to enforce immigration regulations in a way that they could not have done without access to the personal data stored in this digital ecosystem (Morrison, 2020).

Another concern with capital surveillance is the nature in which users' information is stored on a digital platform. If the information is stored any other way, it is typically protected by privacy rights. Medical records are legally protected as some of the most private pieces of data someone could have. The government is restricted from accessing individuals' medical records without due process, for justified reasons. The Health Insurance Portability and Accountability Act (HIPAA) requires patients' sensitive information be kept confidential and not disclosed without the patient's knowledge and consent (US Centers for Disease Control and Prevention, 2022).

However, HIPAA does not necessarily extend to records stored on apps. The Wall Street Journal revealed that cell phone app companies, such as the Instant Heart Rate: HR Monitor and Flo Period & Ovulation Tracker, were sharing users' personal medical information with Facebook (Kennedy, 2020). Imagine if law enforcement attempted to pay Flo to surveil information for prosecution in the same way they have done with Clearview AI. Now that abortion is criminalized or severally restricted in several states after the recent ruling in Dobbs v. Jackson Women's Health Organization (2022), many users of these apps are concerned their personal data could be used against them if they were suspected of having an abortion (Korn et al., 2022).
What is disturbing about this situation is the only reason that HIPAA would not apply and protect the potential defendant's privacy is because the information is stored on an app. Generally, "disclosures for purposes not related to health care, such as disclosures to law enforcement officials, are permitted only in narrow circumstances tailored to protect the individual's privacy and support their access to health care, including abortion care" (HHS, 2022). Even so, the U.S. Department of Health and Human Services (HHS) felt compelled to issue a warning, explicitly stating, "The HIPAA Rules generally *do not* protect the privacy or security of your health information when it is accessed through or stored on your personal cell phones or tablets" (HHS, 2022). They stated HIPAA rules do not protect the privacy of internet search history, information voluntarily shared online, or geographic location information.

Because the methods in which we store our personal data have changed with evolving technology and new societal needs, conveniences, and customs, antiquated privacy laws need to be updated. Users should not be penalized for adapting to modern times, particularly when active and effective participation in society, for everything from using public transportation to going to the doctor, requires use of these digital technologies. For these reasons, lawmakers need to address capital surveillance's intrusive role in data collection and criminal prosecution.

III. Policy Option One: Applying our understanding of privacy in the physical world to the digital world by looking to the nature of the data and not the source

There is an inherent public trust in technology corporations, such as Google and Facebook, as society becomes increasingly dependent on them to communicate, research, and simply participate in everyday life. When protecting privacy rights in the expanding digital ecosystem from legal overreach, lawmakers should look to case law in order to create cognizant policy that awards online data the same kind of protection it would have in the physical world (i.e., recognizing the *nature* of the data, not simply where the information is stored).

That being said, it can be generally understood that not all data a user posts online should be considered private. The challenge is for lawmakers to determine and agree upon digital equivalents of physical world privacy rights, clearly defining what data is considered private and what modes of storage are considered inaccessible to law enforcement without due process. Any policies should be designed to be very nimble as they will likely need regular updating considering the nature of constant change of technology and the digital world.

The case United States v. Warshak (2010), in which law enforcement officers tried to compel a defendant's emails without a warrant, provides insight. The Court held that emails are private and cannot be searched because they are the digital equivalent of a letter and it is reasonable to assure the contents of one's mail are private. Using this as an example, lawmakers should look at what the law has said in the past on the extent of people's privacy rights regarding their physical data and apply these legal concepts to data that is collected virtually.

If we treat digital data the same way we treat physical world data, and apply the same laws to them, then more protections can be put into place, preventing capital surveillance from taking advantage of users' privacy rights, and safeguarding well-established privacy laws.

IV. Policy Option Two: A standard definition of reasonableness

The best way to enforce the right to privacy is to create and enforce a standard definition of "reasonable expectation" of privacy. Perhaps this definition can incorporate asking, "Is the real world

equivalent of this private?" As stated earlier, case law has hinted at standards as to when electronic data should not be shared because the real world equivalent of that data would be protected by privacy expectations.

Generally, one potential definition of a reasonable expectation of privacy might entail the question, "Can the general public easily access this information?" This standard also reinforces rights protected in American common law. When an individual shares their information with another person or service, they forfeit it to the general public, even if it is just a few people. On the other hand, when an individual logs information on an app on their password-protected cell phone, that information is not accessible to the general public.

V. Conclusion

Capital surveillance is the process of surveilling all of a user's data, collecting it, and sharing or selling it to a third party. Governments should not be allowed to buy data collected by capital surveillance without judicial safeguards because data collected by capital surveillance violates user's reasonable privacy expectations. Not only does this practice run afoul of human rights, it is difficult to hold technology companies accountable due to inconsistent national laws and vague policies. By drafting laws framed around the question, "If this information was not on a smartphone, would it be considered protected by established privacy rights?", lawmakers can make consistent, cognizant laws that protect users' data from unfair and unforeseeable practices.

References

Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002). https://casetext.com/case/ashcroft-v-free-speech-coalition?q=Ashcroft%20v.%20Free%20Speech%20Coalition,%20535%20U.S.%20234%20(2002)&sort=relevance&p=1&type=case

Auxier, Brooke. "5 Things to Know about Americans and Their Smart Speakers." Pew Research Center. Pew Research Center, November 21, 2019. https://www.pewresearch.org/fact-tank/2019/11/21/5-things-to-know-about-americans-and-their-smart-speakers/

Dobbs v. Jackson Women's Health Organization, 597 U.S. (2022). https://www.supremecourt.gov/opinions/21pdf/19-1392_6j37.pdf

Fingas, Jon. "Law Enforcement is Using a Facial Recognition App with Huge Privacy Issues." Engadget, January 18, 2020. https://www.engadget.com/2020-01-18-law-enforcement-using-clearwater-ai-facial-recognition.html

Hauser, Christine. "Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing." New York Times, October 3, 2018. https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html?auth=login-google1tap&login=google1tap

Kennedy, Lindsey. "Surveillance Capitalism: An Outlook on the Rise of Data Capital." Best Online Reviews, March 25, 2020. https://www.bestonlinereviews.com/vpn/surveillance-capitalism/

Koch, Lee. "What is the Third Party Doctrine?" Koch Law, July 22, 2022. https://www.nydefensecounsel.com/what-is-the-third-party-doctrine/

Korn, J. and Duffy, C. "Search Histories, Location Data, Text Messages: How Personal Data Could Be Used to Enforce Anti-Abortion Laws." CNN, June 24, 2022. https://www.cnn.com/2022/06/24/tech/abortion-laws-data-privacy/index.html

Legal Information Institute. "Fourth Amendment." www.law.cornell.edu/constitution/fourth_amendment

Legal Information Institute. "Probable Cause." https://www.law.cornell.edu/wex/probable_cause

Morrison, Sara. "A Surprising Number of Government Agencies Buy Cell Phone Location Data. Lawmakers Want to Know Why." Vox, December 2, 2020. https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel

United Nations. "Universal Declaration of Human Rights." United Nations, 1948. www.un.org/en/universal-declaration-human-rights/

United States Centers for Disease Control and Prevention. "Health Insurance Portability and Accountability Act of 1966 (HIPAA). https://www.cdc.gov/phlp/publications/topic/hipaa.html

United States Department of Health and Human Services. "HHS Issues Guidance to Protect Patient Privacy in Wake of Supreme Court Decision on Roe." June 29, 2022. Press Release. https://www.hhs.gov/about/news/2022/06/29/hhs-issues-guidance-to-protect-patient-privacy-in-wake-of-supreme-court-decision-on-roe.html

United States v. Jones, 565 U.S. 400 (2012). https://casetext.com/case/united-states-v-jones-1419?

United States v. Warshak, 631 U.S. 266 (2010). https://casetext.com/case/us-v-warshak-27

Shayna Koczur is an attorney from New Jersey, currently working as a Law Clerk. She graduated Brooklyn Law school in 2021. Prior to graduation, Shayna interned at the Brooklyn District Attorneys' office and Union County Prosecutor's office. She has been published by the Fletcher Forum of World Affairs and by the International Affairs Forum. Prior to law school, Shayna graduated from Bard College with a degree in Global Studies, where her thesis was selected to be presented at St. Petersburg State University in 2018. She has a strong interest in criminal law, international law, and constitutional law.

Acknowledgements

This article is dedicated to one of my best friends, Eamon. He was a brilliant software engineer, but an even better friend. His support made me the attorney I am today.