ASA Research Note

AN ETHICAL APPROACH TO BIG DATA SURVEILLANCE

AUTHOR: Shouyang Wang

PUBLISHED: June, 2022

WRITTEN: Feb. 2021

KEYWORDS: Privacy; Surveillance; Fourth Amendment; Metadata; Mass Surveillance

ABSTRACT: This paper discusses the trade-offs between personal privacy and national security. Through the lens of various philosophical theories, constitutional rights, and judicial rulings, the paper examines how as the surveillance level goes up, the ethical constraints should gradually move from a consequentialist approach to a deontological one.

The trade-off between personal privacy and national security has been one of the most controversial topics due to various invasive government surveillance programs. In the context of post-9/11 America, this paper demonstrates the necessity of privacy and proposes an ethical framework that the U.S. government must enforce when conducting mass surveillance. Based on various philosophical theories, constitutional rights, and judicial rulings, the framework is ethical in nature to ensure an optimized balance between individual privacy and government monitoring.

On September 11, 2001, radical terrorists murdered thousands of innocent people when they crashed the hijacked planes. The incident was a watershed moment for the way intelligence agencies approach national security. In fear of "terrorists among us,"[1] Congress passed *The Patriot Act* to make it "easier for the government to spy on ordinary Americans by expanding the authority to monitor phone and email communications."[2] The abrupt revision of the nation's surveillance laws is justified on the grounds of preventing terrorist activities. During the hearing on *U.S. Federal Efforts to Combat Terrorism* in 2001, the attorney general reasoned that the prevention of terrorist plots could "avert the death or serious injury of tens of thousands of Americans." [3]

Big data surveillance entails an intricate network of problems that are often morally and legally ambiguous. National security and personal privacy are often entangled in a twisted knot that results in many dilemmas. An extreme approach can be detrimental to both individual and national interests. Context and critical thinking matter when dealing with such delicate programs.

It is justifiable that the government needs an organization like the National Security Agency (NSA) to collect critical information that involves national interests. It is somewhat deceptive that the media portrays the NSA as the equivalent of the egregious Big Brother – a symbol that reflects the totalitarian nature of the Soviet regime. The NSA is by law accountable to the Foreign Intelligence Surveillance Court, the legislative branch, and the executive branch.[4] The principle of checks and

Copyright © 2022, ASA Institute for Risk and Innovation

balances safeguards that no agency is above the law. Many people compare the intensity of the NSA surveillance to the dystopian nightmare described in George Orwell's novel *Nineteen Eighty-Four*. Such an exaggerated claim is not only misleading. It instills a sense of mistrust in federal agencies while fostering more misunderstanding.

However, some criticisms toward surveillance programs are valid. Moore asserts that "a right to privacy is a right to control access to, use of, places, bodies, and personal information."[5] Radical surveillance advocates often argue that the telephony metadata NSA collected is not personal information. In *Smith v. Maryland*, the Court ruled that "the right to privacy Americans expect in phone conversations did not extend to the mere record of those calls." [6] Hence, the NSA has the legal grounds to collect metadata about U.S. citizens without violating the Fourth Amendment. Such an argument does not hold water under scrutiny. When the Supreme Court made the ruling in 1979, nobody could have foreseen the power of big data analytics and surveillance technology. NSA's mass data collection is fundamentally different from the Smith case regarding the intensity of the surveillance and the unprecedented methods being employed. In the modern age, people have no choice but to share metadata with third parties when utilizing technology. It is sophism - seemingly plausible but fallacious to contend that metadata is not private information because users "voluntarily" surrender it to phone companies. Rationalizing the very fact that people do not have absolute control when a third party is involved is not only unconstitutional but unethical. Protecting citizens from unreasonable searches is the quintessential power of the Fourth Amendment.

The *United States v. Moalin* case concludes that "the government may have violated the Fourth Amendment when it collected the telephony metadata of millions of Americans."[7] Metadata is sensitive data that convey personal information. By knowing who a person contacts, the system can build up profiles of millions of people based on metadata alone. It identifies your social circle, and it gives clues about your private life. The main concern regarding the subject matter does not stem from whether we have valid allegations to substantiate that the current administration is abusing the data. The issue stems from the fact that any existing or future government official can misuse the technology if we do not hold them accountable. The more privacy we give up, the closer we are to the Orwellian society. Countless real-world examples, such as the human tragedies that happened in North Korea, China under Mao, and the former Soviet Union, have warned us about the danger of giving up privacy for "a good cause."

The issue then arises, how do we set the ethical constraints on mass surveillance to ensure the safety of the American people while upholding the right to privacy? Two main ethical frameworks can be applied to the subject matter. Consequentialists put a "strong emphasis on the results of actions," while deontologists may argue that "the intrinsic good and evil of consequences are irrelevant to determining what is morally right or wrong."[8] In layman's terms, a consequentialist would argue that surveillance is good if the result is good. A deontologist would argue that surveillance is bad because it violates privacy regardless of the outcome. A moderate consequentialist or deontologist would reason that it matters how we do things, but consequences matter as well. We will incorporate both frameworks when dealing with government monitoring because not all surveillance is created equal.

Copyright © 2022, ASA Institute for Risk and Innovation

Overt surveillance is "conducted in the open with the intent of being seen."[9] For instance, CCTV security cameras are installed in crowded public areas for crime prevention. This type of non-discriminating surveillance is viewed as less invasive because being in public means having a lower degree of privacy by default. Admittedly, particular individuals won't be comfortable with the installation. Albeit at the expense of some people's privacy or comfort, the consequentialist appeal to the overall increased security is often justified. However, this is not always the case.

Ryberg argues that overt surveillance tools such as CCTV can be compared to an old lady "who spends her time gazing out onto the street" observing passersby.[10] The old lady's action is not illegal or ethically wrong, and she is by no means violating the privacy of others. Hence, if we replace the old lady with a camera, there is nothing fundamentally invasive about the CCTV systems. Such an argument becomes problematic as the intensity of the surveillance goes up. Imagine having a prodigious number of such old ladies living in the city, keeping track of what they observe every day. It is analogous to having a myriad of CCTV cameras installed in a public place interconnected to report any peculiar behaviors to the authorities. It is suppressing because such implementation transforms the public area into an enormous prison where the guards are always watching. How can we possibly feel a sense of privacy living in prison?

Hence, despite the overt nature of such surveillance, the government must provide transparent and valid reasons to do so while having approval from the majority of citizens living in the area. Once a new surveillance tool is installed, the effectiveness of the device needs to be evaluated regularly. For instance, a camera installed on public security grounds should be removed if comprehensive studies demonstrate that the implementation does not reduce violent crimes. Similarly, it is not logically valid to add more security cameras to an area with a low crime rate. One CNN report shows that "China is installing surveillance cameras outside people's front doors"[11] to stop the spread of the coronavirus. The report indicates that the camera is placed directly outside of a residence's front door – technically a public place.

As the intensity of the surveillance goes up, the ethical constraints should gradually move from a consequentialist approach to a deontological one. In other words, the consequence is irrelevant if the means to achieve such a result is highly unethical and invasive. It is a matter of principle when the right to privacy is violated to a high degree. If we don't implement such ethical constraints on the U.S. government, it is merely a matter of time that the proliferation of surveillance tools poses a threat to our personal freedom.

Unlike overt surveillance, covert surveillance is conducted without the target's knowledge. The privacy issue arises when an agency starts targeting not just criminals but ordinary citizens as well. Federal agencies often justify the collection of bulk metadata "by pointing to the prevention of terrorism, crime and child pornography, even if these aren't always the real reasons."[12]

On top of that, there is not yet a comprehensive study on the mass surveillance program that indicates such a method is useful for counterterrorism. Quite the opposite – a detailed analysis of more than 200 terrorists who were convicted shows that "traditional investigative methods provided

Copyright © 2022, ASA Institute for Risk and Innovation

the initial impetus for investigations in the majority of cases, while the contribution of NSA's bulk surveillance programs to these cases was minimal."[13] In *Klayman v. Obama*, Senior Judge Richard Leon reasoned that the metadata the NSA collected "infringes on that degree of privacy that the Founders enshrined in the Fourth Amendment," and he has "serious doubts about the efficacy of the program."[14]

When operating within such domains, it is appropriate to prioritize a moderate to extreme deontological approach. The reason is that the Fourth Amendment is a moral principle and legal line that can't be crossed. Covert programs can be highly invasive to ordinary Americans due to the clandestine nature. As mentioned previously, *Smith v. Maryland* is not an excuse for bypassing the Fourth Amendment because we are living in a different world. Just like a military strategist would not treat a battle in which swords are used as the primary weapon the same way as nuclear warfare, law professionals must interpret the Fourth Amendment in a way that adjusts to the digital age to keep intelligence agencies accountable. As Justice Sotomayor reasoned in the *United States v. Jones* ruling:

> *"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."*[15]

If we don't draw the line here, it's not just the Fourth Amendment that will be violated. If we know we are being monitored constantly, can we honestly say that Americans have the freedom of speech or freedom of any kind?

SOURCES

[1] Roos, Dave. "5 Ways 9/11 Changed America." HISTORY, 1 Sept. 2020, <www.history.com/news/september-11-changes-america>. Accessed Feb. 2021.

[2] American Civil Liberties Union. "Surveillance under the Patriot Act." American Civil Liberties Union, 2011, <www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act>. Accessed Feb. 2021.

[3] Ashcroft, John. Statement of Attorney General John Ashcroft before the United States Senate Committee on Appropriations Subcommittee on Commerce, Justice, and State, the Judiciary, and Related Agencies Hearing on U.S. Federal Efforts to Combat Terrorism, 2001, <https://www.justice.gov/archive/ag/testimony/2001/ag_statement_05_09_01.htm>. Accessed Feb. 2021.

[4] De, Rajesh. "The NSA and Accountability in an Era of Big Data." Semanticscholar, 2014, <www.semanticscholar.org/paper/The-NSA-and-Accountability-in-an-Era-of-Big-Data-De/c65a075d54b88a1b528dca0dd60a381ece690ddf.> Accessed Feb. 2021.

[5] Moore, Chapters 2, Privacy Rights: Moral and Legal Foundations. 2010. Accessed Feb. 2021.

[6] Rodricks, Dan. "Maryland Case Provides Basis for NSA Surveillance." Baltimoresun.com, 11 Nov. 2013, <www.baltimoresun.com/maryland/bs-xpm-2013-11-11-bs-md-rodricks-1112-20131112-story.html.> Accessed Feb. 2021.

[7] Case No. 10CR4246-JM 08-22-2012 UNITED STATES OF AMERICA, Plaintiff, v. BASAALY MOALIN et al., Defendants. United States v. Moalin, Case No. 10CR4246-JM, (S.D. Cal. Aug. 22, 2012)

[8] Regan, Tom. 2005. "Introduction to Moral Reasoning". Accessed Feb. 2021.

[9] "Surveillance Techniques – Babnick and Associates, LLC." Babnickandassociates.com, <www.babnickandassociates.com/services/business-services/surveillance-techniques/>. Accessed Feb. 2021.

[10] Ryberg, Jesper. "Privacy Rights, Crime Prevention, CCTV, and the Life of Mrs Aremac." Res Publica, vol. 13, no. 2, June 2007, pp. 127–143, 10.1007/s11158-007-9035-x. Accessed Feb. 2021.

Copyright © 2022, ASA Institute for Risk and Innovation

[11] Gan, Nectar. "China Is Installing Surveillance Cameras Outside People's Front Doors ... And Sometimes inside Their Homes." CNN, 27 Apr. 2020, <www.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html>. Accessed Feb. 2021.

[12] Beens, Robert E. G. "Council Post: The State of Mass Surveillance." Forbes, 25 Sept. 2020, <www.forbes.com/sites/forbestechcouncil/2020/09/25/the-state-of-mass-surveillance/?sh=454b4dd5b62d>. Accessed Feb. 2021.

[13] Cahall, Bailey, et al. "Do NSA's Bulk Surveillance Programs Stop Terrorists?" New America, 2019, <www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/>. Accessed Feb. 2

[14] "Federal Judge's Ruling on N.S.A. Lawsuit." <www.nytimes.com, 16 Dec. 2013, archive.nytimes.com/www.nytimes.com/interactive/2013/12/17/us/politics/17nsa-ruling.html>. Accessed Mar. 2021.

[15] "United States v. Jones, 565 U.S. 400 (2012)." Justia Law, 2012, <supreme.justia.com/cases/federal/us/565/400/>. Accessed Feb. 2021.

Copyright © 2022, ASA Institute for Risk and Innovation