ASA Research Note

TECHNOLOGY'S THREAT TO DEMOCRACY

AUTHOR: Katia Vales
PUBLISHED: December 2023
WRITTEN: May 2023

KEYWORDS: Democracy; Biometrics; Privacy; Privacy and Ethics; Regulatory Environment; Governments; Constitutional Rights; Surveillance
ABSTRACT: This paper discusses how advances in technology have not only brought countless benefits to humanity but have also infringed on people's privacy. The author suggests that continuing to use technology to protect the very liberties that the same technology jeopardizes stands as a significant contradiction to the institutions of this country. While it may feel "justified" to use these invasive technologies because of criminal actions, it is vital to consider the bigger picture and think about what it means for citizens to exist in a state of continuous monitoring.

Throughout history, technological advancement has been the critical ingredient of societal progress. Behind each turn of an era existed a catalytic invention that enhanced how people could participate in, communicate with, and educate themselves about the world around them. Civilizations began to flourish exponentially following the advent of major technological innovations such as the printing press, electricity, and, most recently, the internet, which increased people's opportunities to further their self-expression, interests, and identity. However, though technology has markedly improved people's agency and individuality, technology has also created many avenues to infringe on people's privacy and expose their identity beyond their control.

Governments have encouraged and adopted the advancement of such technologies under the veil of protection. Yet, regardless of intent, the use of such technologies is growing more dangerous and more secretive by the day. The various forms of surveillance technology being used by the government are threatening people's privacy and their desire and ability to express themselves in society freely. This is a direct threat to democracy, and such inappropriate use of government power should be considered a violation of the First and Fourth Amendments of the Bill of Rights[1].

Unfortunately, the four doctrines of physical intrusion,[2] as well as other originalist interpretations of the Constitution, have failed to provide people with the protection they deserve. Given the speed and power of technological development, the courts should approach constitutional interpretation with a modern lens that understands the need to draw protective boundaries around the expansive yet invasive reach of technology. Without such a lens, the people lay exposed to the unbridled power of the government in an ever-technologized era.

Much debate exists about how to define privacy. As the word "privacy" is not present within the Bill of Rights, there also exists debate about whether it is, or should be, offered constitutional protection. Some theorists, such as William Parent, believe privacy to be a state or condition that

people voluntarily forfeit in trivial ways each day as they engage in social media, e-commerce, etc. Thus, privacy rights should not be given similar protections as liberty rights[3]. However, other theorists, such as Richard Parker, condemn this view as it ignores any individual capacity for control. Parker believes that privacy involves an individual's ability to control when, where, how, and by whom others can sense any part or aspect of information about them. The word *sensed* here is essential because it encompasses how something can be discovered and thus taken by someone or something – whether by seeing, hearing, touching, etc. This definition, which highlights the non-physical elements of security, should eliminate any uncertainty of privacy protection under the Bill of Rights, namely, the Fourth Amendment, which stands as:

> "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."[4]

Unfortunately, due to the court's emphasis on the physical embodiment and proximate nature of persons and things to be searched and seized, technology's ability to exist in a digital and peripheral landscape has allowed it to propagate just outside the shadows of the law and provide the government room to build covert schemes of control beyond the awareness of the public.

In Chapter 12 of her book, *Privacy, Security, and Accountability*, Strossen criticizes the U.S. government for its tactics of secrecy and its expansive use of technology to conduct surveillance on the American public.[5] She points out that though these tactics are not new, the terrorist attacks of 9/11 propelled the use of surveillance technology to new heights. Moreover, in the almost 10 years since her book, the government's use of technology has only become more invasive and more advanced. A policing technology conference in Dubai in March 2023 showcased hacking software, brain wave readers, facial recognition software, and surveillance technologies for sale to both private entities and governments.[6] Invasive technologies like these, which many believed were only utilized by authoritarian countries like China, are now proliferating across law enforcement agencies worldwide. Trends such as this ring the alarm on how the shift in policing's focus from officers and weaponry to data and software poses a significant danger to people's privacy and raises questions about how nations wield their political power.

A recent example of the U.S. government's use of these invasive technologies occurred after the January 6th, 2021 insurrection in Washington, D.C. To find those who stormed the Capital, law enforcement utilized facial recognition software to detect the trespassing rioters.[7] This was a continuation of a much longer trend - according to a U.S. Government Accountability Office (GAO) report, law enforcement agencies "performed 390,186 database searches to find facial matches for pictures or video of more than 150,000 people between 2011 and 2019." Yet, government searches are not limited to pictures and videos. Recently, with the case of the Golden State Killer, law enforcement exposed their willingness to dive deeper into even more private information of its citizens – their DNA.[8] In the case, the FBI conducted unsanctioned and covert searches of DNA profiles on GEDmatch, FamilyTreeDNA, and MyHeritage, and created new

DNA profiles using forensic profiles to find their match. Not only did these searches violate a few of these companies' privacy policies, but the searches also sparked a debate about the legality of law enforcement's access to an individual's genetic privacy.

Discoveries in DNA collection and identification at the University of Florida make this debate about genetic privacy very timely.[9] Research efforts aimed at using a powerful yet inexpensive tool to gather environmental DNA from everyday elements such as dirt, air, and water have, coincidentally, led to new developments in scientists' ability to capture genetic information about human populations and individuals themselves. Scientists involved in this research immediately understood the dilemma this presented for protecting privacy. Scientists have condemned law enforcement's history of rushing to adopt technologies before establishing sufficient proof that they work or properly analyzing the threats they may pose to the public. The larger academic and research communities' critique of the government's deployment of such technologies highlights a disparity between what law enforcement is allowed to do in the name of public safety versus what is allowed by publicly funded research and private companies.

Each of these examples, from the police tech conference in Dubai to the eDNA discoveries at the University of Florida, demonstrates how the four doctrines that separate virtual and public access from physical intrusion - *knowing exposure, general public use, contraband specific, and assumption of risk*[10] – provide the government immunity from constitutional regulation. The knowing exposure doctrine, which asserts that what a person knowingly exposes to the public is not provided Fourth Amendment protection, casts a vast net of immunity for the government. This doctrine allows the government to track someone's car, use surveillance to spot a protester at a rally, or even scoop up an individual's DNA left at the local lake after a swim. A similarly large net of immunity exists with the assumption of risk doctrine which no longer considers private information provided to a third party. As such, any photo posted to social media or any DNA profile created on a heritage site, can be searched by the government without a warrant. Finally, the doctrine is casting an exceedingly wider net is the public use doctrine. The fact that the designated "government zone" existed in a restricted area away from the rest of the Dubai tech conference[11], underlines the dangerous reality that most policing of technology on display was not reserved for government entities alone. The opposite was true. Therefore, if most of these intrusive police tools can be purchased by everyday individuals, they can be used to watch, listen, and track a given individual or group in public and private places without constitutional regulation under the general public use doctrine.

Unfortunately, these doctrines are not the only things shielding the U.S. government from constitutional law. Another is their secrecy. Just as the government's deployment of surveillance technology has grown more sophisticated, it has also grown more elusive. The public was not informed of the many surveillance programs the NSA, CIA, and other government agencies spawned in the 20 years since 9/11.[12] Instead, the programs were kept hidden from the public and only exposed through document leaks by Edward Snowden, and resulting consequences. Herein lies the problem. How are individuals supposed to protect their privacy, or at the very least, defend their *right* to privacy, if they have no idea what they are protecting against or who? Furthermore, how can

the public feel comfortable expressing themselves freely as participants in society if they cannot trust that such expression is taking place outside the examination of the government? These questions highlight the reality that the government's veiled use of surveillance technology goes beyond infringing on the public's protection from search and seizure under the Fourth Amendment. Their use also directly conflicts with the rights outlined by the First Amendment.

The First Amendment declares that the government cannot hinder the public's freedom of speech, expression, peaceful assembly, or the press. Therefore, not disclosing the purpose and scope of surveillance programs acts as a threat to the First Amendment in two regards. First, it prohibits the press from performing their societal role of providing individuals with the information they need to make informed decisions and ensuring that elected officials remain accountable for the duties of their office and the wishes of the citizens they serve.[13] Without access to information about the surveillance programs, the press cannot educate the public about the impact of such programs and nor ensure the government's use of such technology aligns with the majority opinion of the public. Secondly, if the government can surveil the public and track them as they engage in society, then such power eliminates the "free" aspect of speech, expression, and peaceful assembly outlined in the First Amendment. Though the government may not be *preventing* people from saying or participating in something, if people do not trust how the government may utilize the personal information collected on their communications or activities, then people will begin to retreat to measures of self-censorship. As Adam Moore states in his article, *Privacy: Its Meaning and Value*, "controlling access to ourselves affords individuals the space to develop themselves as they see fit. Such control yields room to grow personally while maintaining autonomy over the course and direction of one's life."[14] Thus, curtailing such control and autonomy will have disadvantages and impacts on individual development and, thus, compounding impacts on the intellectual, creative, and societal progress of our nation.

Many believe this previous statement asserts an extremist view of privacy concerns. Some groups argue that only those who have "something to hide" should be worried about the potential risk of being caught by the government's surveillance initiatives and that those who have "nothing to hide" need not fear the technological tools the government employs to keep them safe. However, though these groups may feel like justice was served for the January 6th rioters or the Golden State Killer and may not be concerned about what the government surveillance programs mean for their privacy, it is vital to consider the bigger picture and think about what it means to constantly be watched – especially when you don't trust the person who is watching. Given the turbulent political climate of today surrounding the Black Lives Matter Movement, LGBTQ+ rights activism, Women's rights activism, and gun safety, citizens from all sides of the political spectrum must consider what it means for the government to be able to track each action or decision citizens made related to these topics. Would they feel just as safe or as free? Would they participate as fully or speak as candidly if they thought no one could know? These are the exact questions that underline how people's sense of personal freedom begins to dissolve as they lose trust and control of their privacy. And this is exactly why there must be greater protections surrounding privacy.

In summary, given the threat that technology-driven policing tools and surveillance programs pose to the constitutional rights of American citizens outlined in the First and Fourth Amendments, it is past time for the court systems to reconsider the validity of the four physical intrusion doctrines. These doctrines are out of touch with the reality of this ever-digitized and accessible world and, as a result, leave U.S. citizens as defenseless victims to the government's addictive abuse of technological progress. The courts must eliminate the *physical* requirement within constitutional interpretation and, instead, apply a more flexible digital and modern context to constitutional analysis. Additionally, the U.S. government must cease the secrecy operations that began before—yet proliferated in—the aftermath of 9/11. Such operations include, but are not limited to, the severe restriction of the government press contact and the Freedom of Information Act (FOIA), the dismissal of lawsuits that challenge illegal actions in the name of the "War on Terror," and the spying on and intimidating of journalists.[15] Though there have been a few bipartisan efforts and court decisions since the Snowden leaks which have established meaningful protections of privacy rights, there is still a lot of work the government must do to repair the public's trust and demonstrate respect for their citizens' privacy and freedom. The civil liberties established and protected by the Constitution symbolize the values upon which the United States was founded. Therefore, to continue to use technology to protect the very liberties that the same technology jeopardizes stands as a significant contradiction to the institutions of this nation.

SOURCES

[1] Library of Congress. (1959). A bill of rights as provided in the ten original amendments to the constitution of the United States in force. https://www.loc.gov/resource/rbpe.24404400/

[2] Slobogin, Christopher. (2010). *Is the Fourth Amendment Relevant in a Technological Age*. https://www.brookings.edu/wp-content/uploads/2016/06/1208_4th_amendment_slobogin.pdf

[3] Moore, Adam. (2003). *Privacy: Its meaning and value*. American Philosophy Quarterly.

[4] Library of Congress. (1959). A bill of rights as provided in the ten original amendments to the constitution of the United States in force. https://www.loc.gov/resource/rbpe.24404400/

[5] Strossen, Nadine. Chapter 12 – Post 9/11 Government Surveillance Suppression Secrecy. *Privacy, Security and Accountability: Ethics, Law and Policy*. Edited by Adam Moore (Rowman & Littlefield, London and New York, 2015).

[6] Mozur, Paul and Satariano, Adam. (March 2023). *A.I., Brain Scans and Cameras: The Spread of Police Surveillance Tech*. The New York Times. https://www.nytimes.com/2023/03/30/technology/police-surveillance-tech-dubai.html

[7] Bhuiyan, Johana. (2021). *Facial Recognition may help find Capitol rioters – but it could harm many others, experts say*. Los Angeles Times. https://www.latimes.com/business/technology/story/2021-02-04/facial-recognition-surveillance-capitol-riot-black-and-brown-communities

[8] Paige, St. John. (2020). *The untold story of how the Golden State Killer was found: A covert operation and private DNA*. Los Angeles Times. https://www.latimes.com/california/story/2020-12-08/man-in-the-window

[9] Brown, Elizabeth Anne. (May 2013). *Your DNA Can Now Be Pull From Thin Air. Privacy Experts Are Worried*. New York Times. https://www.nytimes.com/2023/05/15/science/environmental-dna-ethics-privacy.html

[10] Slobogin, Christopher. (2010). *Is the Fourth Amendment Relevant in a Technological Age*. https://www.brookings.edu/wp-content/uploads/2016/06/1208_4th_amendment_slobogin.pdf

[11] Mozur, Paul and Satariano, Adam. (March 2023). *A.I., Brain Scans and Cameras: The Spread of Police Surveillance Tech*. The New York Times. https://www.nytimes.com/2023/03/30/technology/police-surveillance-tech-dubai.html

[12] Strossen, Nadine. Chapter 12 – Post 9/11 Government Surveillance Suppression Secrecy. *Privacy, Security and Accountability: Ethics, Law and Policy*. Edited by Adam Moore (Rowman & Littlefield, London and New York, 2015).

[13] The U.S. Agency for International Development. *The Role of the Media in Democracy: A Strategic Approach*. https://2017-2020.usaid.gov/sites/default/files/documents/2496/200sbc.pdf

[14] Moore, A. (2003). *Privacy: Its meaning and value*. American Philosophy Quarterly.

[15] Strossen, Nadine. Chapter 12 – Post 9/11 Government Surveillance Suppression Secrecy. *Privacy, Security and Accountability: Ethics, Law and Policy*. Edited by Adam Moore (Rowman & Littlefield, London and New York, 2015).