Privacy in the Digital Polis

Curtis Bristol
Research Assistant

September 2026

UVU GARY R. HERBERT INSTITUTE FOR PUBLIC POLICY
800 W University Pkwy, Orem, UT 84058
801-558-9371 | uvu.edu/herbertinstitute/

Introduction

The Greek word for a city-state, polis, while not commonly used today, conveys a concept that is relevant to the conversation of modern-day privacy. The term polis may be more recognizable as the root for many of the words used in everyday conversations about governance, society, and citizenship, e.g., police, policy, and politics.[1] It was in these Greek city-states, with their sense of community and civic engagement, that many of the most fundamental questions and paradoxes of society and governance were first examined and discussed in detail, including the question of security vs liberty.[2] Stemming from this tension is the crucial question, where is the proper place and emphasis of privacy, both in society and law?

Technological Improvements, Privacy Implications

While modern technology has advanced astronomically since the days of the original polis, this technological improvement has not been accompanied by a resolution of the security and liberty paradox, nor a simplification of privacy concerns. Rather, technology has drastically complicated these matters. Below are a few examples of recent technologies and a brief summary of their potential to tip the scales in favor of security at the risk of compromising privacy:

License Plate Readers (LPRs)



License plate readers are cameras designed and positioned to capture images of vehicles and digitize the license plate information in real time. Certain LPR systems take note of other vehicle characteristics such as if the vehicle has paper license plates or any vehicle modifications. In addition to the level of detail, the scope of such surveillance can be surprising. For example, a large LPR provider, FLOCK, states that their system "provide[s] comprehensive access to data, giving officers leads from other LPR cameras at the local, state, and nationwide levels. This allows law enforcement to monitor the vehicle movements of suspected offenders regardless of their location."[3]

Video Cameras

For the purposes of this discussion of public security and individual liberty, this section refers specifically to video cameras owned and operated by the government, primarily by local governments and police departments. FLOCK, for example, offers video cameras with AI-powered instant-alert systems, human detection (though not individual characteristics), powerful AI search features, and a system that coordinates with LPRs and other security and surveillance products.

Mobile Security Trailers

FLOCK's website advertises its "mobile security trailers" with the caption, "Place coverage where you need it most without wiring or permits."[4] These portable camera trailers operate independently of any infrastructure and integrate into the customer's platform for "total visibility."[5] Of particular note is the way that this technology circumvents typical permitting requirements and how its providers market that capacity as one of its main strengths. This could be seen as efficiently streamlining the efforts of law enforcement officers to keep their communities safe by cutting through bureaucratic red tape, or conversely, it could be viewed as an alarming and blatant disregard for privacy protections and individual liberty.

Video Doorbell Cameras



Video doorbell cameras are commonly used in neighborhoods to dissuade and catch "porch pirates." They allow individuals to see who comes to their door, and even enable them to communicate remotely with visitors at their door. However, much like the other technologies mentioned, the convenience and benefit they provide are not without privacy ramifications. For example, the industry leader of video doorbell cameras, Ring, ran a 2026 superbowl commercial showing how AI search functions that are built into their cameras (and are on by default), can help individuals locate a lost pet throughout their neighborhood. The concerned family member simply enters a brief description of the lost dog into the "search party" feature, and an AI-powered search is run using all the other Ring cameras in the network that haven't had the feature specifically turned off by their individual owners. The neighborhood camera system, working in unison, then finds the dog or cat quickly and efficiently.

The Electronic Frontier Foundation (EFF), a non-profit dedicated to digital privacy, free speech, and innovation, highlights how this commercial uses a heartwarming end to justify means that should be incredibly concerning for privacy-minded individuals. The EFF article also highlights some of the past complications Ring has had with personal data and privacy, including giving law enforcement agencies information without being served warrants, creating partnerships with companies such as FLOCK that partner heavily with the police, and creating a way for officers to ask users directly for their footage. With face-recognition software already in use with Ring's "Familiar Faces" feature, the concerns of individualized surveillance en masse increases.[6]

Car Infotainment Systems

Vehicle infotainment systems are technology hubs for music, navigation, smart phone integration, and general increased convenience such as climate control. These systems record and store a great deal of information from driving habits—speeds driven, sharp turning, hard braking, and locations driven—to phone contacts and messages.[7] Newer vehicles contain almost a virtual clone of an individual's cell phone, aggregated with the vehicle-specific data. The laws regarding vehicular data are more lax than in other data privacy fields. This information is being collected and collated by data brokers and sold to private and state actors, such as insurance companies and law enforcement agencies.[8]

Cell Phones



Cell phones have become an indisputable staple in everyday life, but the same features that make life so convenient can also jeopardize anonymity and privacy. Being aware of the privacy implications can be helpful to mitigate these harmful effects.

Similar to vehicle infotainment concerns, one major way cell phones threaten privacy is through location services. According to the EFF, "Dozens of data brokers collect information about the precise movements of hundreds of millions of people without their knowledge or meaningful consent. They sell this data to a variety of private and state actors. This extremely sensitive information can reveal where we live and work, who we associate with, and where we worship, protest, and seek medical care." The article states that data brokers primarily get this data from third party apps, e.g. weather apps, coupon apps, navigation apps, etc.[9]

Aggregated Data and Real-Life Examples

The data collected by the above technologies and others is dual natured with both alluring security benefits and worrying threats to liberty. The pros and cons of each of these individual technologies collecting isolated pieces of information (such as driving habits, text messages, or doorbell footage), increase dramatically as they are aggregated into a vast, rigorous network. For example, a Fitbit reading and a video camera's footage led to the arrest of a ninety-year-old man for the alleged killing of his stepdaughter with an axe or hatchet. He died in prison before going to trial.[10] In another example, a warrant allowing the police to access Google's location services around the time and location of a crime (also known as a geofence warrant), led to the wrong man being arrested for a murder. He was released after six days in jail, but lost his job and car, and was forced to drop out of college as a result.[11] In some cases, the aggregation of data collected through various technologies helps catch the wrongdoers; in others it incarcerates the wrong individual. The degree to which law and society will accept these risks and benefits remains undetermined. While the specific technological advancements currently in question are novel, innovation in both technology and ideology leading to changes to the law's view of privacy is not.

Past Views of Privacy—An Overview of Landmark Supreme Court Cases

A discussion on the current state of privacy and the liberty vs. security paradox would be incomplete without a brief overview of how this conversation has played out and evolved in the US over the past 100 years. The priorities of a democratic society determine its laws, and the national voice, both of the people and the government, can often be determined retroactively by studying the rulings of judges interpreting those laws. The following is a quick synopsis of many of the landmark US Supreme Court cases regarding privacy.



Olmstead v. US (1928)

In 1928, in the middle of Prohibition, Roy Olmstead was suspected of being a bootlegger by federal agents. These agents, without attaining any approval from the courts, installed wiretaps in his office as well as in the streets outside his house. Olmsted was then convicted with evidence obtained from the wiretapping equipment.

In reviewing the case, the Supreme Court held that such wiretapping was not unconstitutional, since the Fourth Amendment's language refers to an "official search and seizure of [one's] person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' [one's property around their home] for the purpose of making a seizure."[12]

Griswold v. Connecticut (1965)

In 1897, a law was passed in Connecticut that outlawed the use of any form of contraceptives. Roughly sixty years later, the head of Planned Parenthood in Connecticut, Estelle Griswold, with the help of a gynecologist from the Yale School of Medicine, opened a birth control clinic in one of Connecticut's main cities. They planned to use the clinic to challenge the validity of the law banning contraceptives. They were arrested and convicted, with higher state courts affirming their convictions. When it reached the Supreme Court, however, the ruling was overturned under the reasoning that a right to privacy existed in the "penumbras" (light shadows/zones) of the First, Third, Fourth, and Ninth Amendments (meaning the right to privacy was hinted at and implicitly present in the aforementioned amendments), and was applied to the states by the Fourteenth. Some of the Justices joined the majority but wrote concurring opinions that simply stated there was no need for imaginary penumbras; the right of privacy could be found in the Ninth and/or Fourteenth amendment.[13]

Katz v. US (1967)

Almost forty years after Olmstead v. US, a very similar case came before the Supreme Court. Federal agents suspected that Charles Katz was relaying illegal gambling information via phone to clients that he had in other states. The agents placed an eavesdropping device on the outside of the public payphone Katz used. The recordings of his side of the conversation led to Katz receiving an eight-count indictment of illegally transmitting gambling information. The Supreme Court overturned the rulings of the lower courts who upheld the conviction, as well as its own ruling from roughly forty years prior with Olmstead v. US. Here is a notable shift from the Court's concept of the Fourth Amendment protecting only against physical intrusions to the famous line from this case, "The Fourth Amendment protects people, not places." In addition, the concept of a reasonable expectation of privacy began in a concurring opinion of this case.[14]

Smith v. Maryland (1979)

In 1975, Patricia McDonough was robbed in Baltimore. She gave the police a description of the robber and the vehicle she thought he was driving. Over the next few days she received threatening phone calls, with one ending with the caller telling her to stand on her front porch. She did so and saw the same vehicle that she had identified as the robber's drive past. A few more days passed and the police located the vehicle in her neighborhood, ran the license plate, and discovered the car was registered to Michael Smith. The police then contacted the telephone company and asked them to record the numbers dialed from the phone at Smith's home via a device called a pen register. The next day, the device recorded a call from Smith's home to Patricia's, and the police used that to obtain a warrant and search Smith's home. He was arrested and put in a lineup where Patricia identified him as the robber. The Supreme Court upheld Smith's conviction on the grounds that an individual must believe that the government violated their reasonable expectation of privacy, and that the reasonable expectation of privacy doesn't apply to information voluntarily and knowingly given away, including to a third party. This applies to numbers dialed on a telephone since such numbers are known to be used by the phone companies.[15]

Riley v. California (2014)

In 2009, David Riley was involved in a gang shooting. He and the others fled the scene, but Riley was pulled over a few weeks later for driving with a suspended license registration. The car was searched prior to impoundment, as was the policy. The officer found two firearms and arrested Riley. Upon arrest, Riley had his cell phone in his pocket, and an officer took it and went through it, finding photos and videos that implicated Riley as a gang member and led to Riley getting convicted. The case reached the Supreme Court, which unanimously held that the warrantless search of a cell phone is unconstitutional.[16]

Carpenter v. US (2018)

In 2011, four men were arrested in connection with a number of armed robberies. One of the men confessed, and volunteered his phone number and the phone numbers of the other three men to the FBI. The FBI used these numbers to apply for orders from magistrate judges to obtain "transactional" records for each of the three cell phone numbers. They received the orders based under the Stored Communications Act. Timothy Carpenter, one of the three men, was then convicted based on cell-site evidence obtained. The Supreme Court, in a 5-4 decision, held that the FBI's obtaining of the cell-site information was a search, and since it was warrantless, it was not constitutional. The majority cited the increasing technological impacts on reasonable expectations of privacy, and that new circumstances of privacy rights can't always fit nicely into old precedents in this digital age.[17]

Looking Forward



As demonstrated, the legal view of privacy rights has changed drastically over the past century, with the status quo now leaning closer to individual privacy and liberty. However, the last case in the list, Carpenter, was only eight years ago, and already technology has advanced dramatically. How well would these rules and principles hold if the circumstances of these cases were updated to reflect current technology? What constitutes a reasonable expectation of privacy in a world where doorbells, cars, cellphones, and highway cameras can create a heavy quilt of convenient, comfortable surveillance? Legislators and the courts will have to put specific answers in place; with increasing innovation and the already tenuous balance between personal privacy and security, the current language and precedents are simply not sufficient." Jackie O'Neil, writing for *Harvard Law Review* stated, referring to two circuit court's polar opposite rulings on the constitutionality of geofence warrants, "This development dispelled any lingering delusions that current Fourth Amendment doctrine is a useful and coherent fit for private mass-surveillance technology."[18]

O'Neil's assessment aptly applies to public as well as private technologies. The current understanding and application of legal precedents and theories in response to modern-day privacy questions is inadequate. New legislation representing and protecting the interests of the people will have to determine and define the balance between security and liberty on this digital front. Waiting for courts to solve each issue as they come up is not a viable or democratic option. Leaving this matter to chance and simply seeing which way it goes would be disastrous. Much like in the ancient Greek polis, citizens must become civically engaged. The balance between security and liberty should be discussed and decided from the bottom up. The citizenry should empower representatives who support their views. The best outcome requires that everyone realizes both that the result of this debate will greatly impact their everyday lives, and that they truly have a voice in which way it ends.

Protecting Liberty in the Digital Age Example of Star Action: Utah's Efforts in Digital Privacy

Utah has responded to the unique challenges to privacy and liberty in the digital age with a variety of legislation and other government actions, including—

- Creating the state's Office of Data Privacy in 2024, and appointing the state's first chief privacy officer[19]
- Combatting increased online scamming, impersonations, and excessive data sharing, all while streamlining identity verification through State Endorsed Digital Identity (SEDI)
    - What is SEDI? SEDI is Utah's framework for digital identity in which the individual owns their identity and the state endorses key credentials, such as age, name, etc. The individual can efficiently and securely verify his or her identity online or in person while disclosing the least amount of information required for the specific service. The original bill authorizing SEDI was passed in 2025, with enabling legislation passed in the 2026 legislative session.[20]
- Passing the "nation's strongest digital identity legislation"[21] with its "Digital Identity Bill of Rights," (SB 275, passed in 2026. Attached below is a copy of the Digital Identity Bill of Rights).
    - In an interview with Utah Representative Paul Cutler, the House sponsor of SB 275, he stated that if he could speak with someone who hadn't heard anything about digital identity until now, the first thing he would say is, "This is really important, something you should learn about."[22]
    - He went on to describe the importance of changing the way we verify identity digitally, and highlighted the crucial role the rights listed in the Digital Identity Bill of Rights play.
    - Some of the specific rights and protections he emphasized include the right to still use physical identification, the protection against the state forcing someone to hand over their phone or digital device to verify their identity.[23]

Digital Identity Bill of Rights

The following rights constitute the digital identity bill of rights in this state:

1. An individual possesses an individual identity innate to the individual's existence and independent of the state, which identity is fundamental and inalienable.
2. An individual has a right to the management and control of the individual's digital identity to protect individual privacy.
3. An individual has a right to choose, receive, and use a physical form of identity assertion that is endorsed by the state.
4. An individual has a right to not be compelled by the state to possess, use, or rely upon a digital form of identity assertion in place of a physical form of identity assertion that is endorsed by the state.
5. An individual has a right to state endorsement of the individual's digital identity upon meeting objective, uniform standards for eligibility and verification established by law, and a right to not have such endorsement arbitrarily or discriminatorily withheld or revoked.
6. An individual has a right to have the state's operation of digital identity systems governed by clear standards established by the Legislature, including for eligibility, issuance, endorsement, acceptance, revocation, or interoperability of digital identity assertions.
7. An individual has a right to transparency in the design and operation of a state digital identity, including the right to access, read, and review the standards and technical specifications upon which the state digital identity is built and operates.
8. An individual has the right to choose what identity attributes are disclosed by the individual's state digital identity in accordance with standards established by the Legislature.
9. An individual has the right to any service or benefit to which the individual is otherwise lawfully entitled based on the individual's choice of a lawful format or means of identity assertion without denial, diminishment, or condition.
10. An individual has a right to be free from surveillance, profiling, tracking, or persistent monitoring of the individual's assertions of digital identity by the state, except as authorized by law.
11. An individual has a right to not be required by the state to surrender the individual's device in order to present the individual's digital identity.

Endnotes

1. Merriam-Webster, s.v. "Polis," accessed June 16, 2026, https://www.merriam-webster.com/dictionary/polis.
2. Stone, Deborah, "Policy Paradox: The Art of Political Decision Making," chap. 5, *Liberty* (New York: W.W. Norton & Company, 2012).
3. Flock Safety, "LPR Cameras for Law Enforcement," accessed June 16, 2026, https://www.flocksafety.com/blog/lpr-cameras-for-law-enforcement.
4. Flock Safety, "Video Cameras," accessed June 16, 2026, https://www.flocksafety.com/products/video-cameras.
5. Ibid.
6. Electronic Frontier Foundation, "No One, Including Our Furry Friends, Will Be Safer in Ring's Surveillance Nightmare," February 2026, accessed June 16, 2026, https://www.eff.org/deeplinks/2026/02/no-one-including-our-furry-friends-will-be-safer-rings-surveillance-nightmare-0.
7. Teague, Chris, "Your Car Is Spying on You and You Probably Agreed to It," *CBT News*, accessed June 16, 2026, https://www.cbtnews.com/your-car-is-spying-on-you-and-you-probably-agreed-to-it/.
8. *Consumer Reports*, "How to Stop Your Car from Collecting and Sharing Driving Data," accessed June 16, 2026, https://www.consumerreports.org/electronics/personal-information/how-to-stop-your-car-from-collecting-sharing-driving-data-a1233378612/.
9. Electronic Frontier Foundation, "Location Data Brokers," accessed June 16, 2026, https://www.eff.org/issues/location-data-brokers.
10. KTVU Staff, "91-Year-Old San Jose Man Accused in Killing Where Fitbit Gave Clues Dies," *KTVU*, accessed June 16, 2026, https://www.ktvu.com/news/91-year-old-san-jose-man-accused-in-killing-where-fitbit-gave-clues-dies.
11. Smith, Michael T, "The Fourth Amendment and Digital Surveillance," (article title may vary), *Missouri Law Review,* 90, no. 4 (2025), accessed June 16, 2026, https://scholarship.law.missouri.edu/mlr/vol90/iss4/10/.
12. Olmstead v. United States, 277 U.S. 438 (1928), Oyez, accessed June 16, 2026, https://supreme.justia.com/cases/federal/us/277/438/.
13. Griswold v. Connecticut, 381 U.S. 479 (1965), Oyez, accessed June 16, 2026, https://www.oyez.org/cases/1964/496.
14. Katz v. United States, 389 U.S. 347 (1967), Oyez, accessed June 16, 2026, https://www.oyez.org/cases/1967/35.
15. Smith v. Maryland, 442 U.S. 735 (1979), Oyez, accessed June 16, 2026, https://www.oyez.org/cases/1978/78-5374.
16. Riley v. California, 573 U.S. 373 (2014), Oyez, accessed June 16, 2026, https://www.oyez.org/cases/2013/13-132.
17. Carpenter v. United States, 585 U.S. ___ (2018), Oyez, accessed June 16, 2026, https://www.oyez.org/cases/2017/16-402.
18. O'Neil, Jackie, "Much Ado About Geofence Warrants." *Harvard Law Review Blog*, February 18, 2025, https://harvardlawreview.org/blog/2025/02/much-ado-about-geofence-warrants/
19. Utah State Archives, "Privacy Bill FAQ," June 11, 2024, accessed June 16, 2026, https://archives.utah.gov/2024/06/11/privacy-bill-faq/.
20. Stanley, Jay, "Utah's Digital ID Law," *American Civil Liberties Union*, accessed June 16, 2026, https://www.aclu.org/news/privacy-technology/utah-digital-id-law.
21. Ibid.
22. Interview with Representative Cutler, April 22, 2026.
23. Ibid.

Gary R. Herbert Institute Staff and Advisors

LEADERSHIP TEAM
Gary R. Herbert, Founder, 17th Governor of Utah
Justin Jones, MS, Senior Director
David Connelly, PhD, Research Director, Associate Professor, History/Political Science
Karen Gill, Events Director
Jim Moss, EdD, JD, Professional in Residence, Constitutional Federalism Initiative
Erik Nystul, MPA, Program Director, Government Internships
Becca Aylworth Wright, Director of Academic Engagement and Publications
McKenna Johnston, Admin Support III
Gabriela Romero Melgar, Admin Support III

ASSOCIATED LEADERS
Liv Moffat, Development Director, Herbert Foundation
Roland Griffin, Director of Development, Academic Affairs

FACULTY FELLOWS
Tara B. B. Bishop, PhD, Assist. Prof. Earth Science / Enviro Mgmt., Earth Sciences
George Rudolph, PhD, Chair/Professor, Computer Science
Majid Memari, PhD, Assistant Professor, Computer Science
David Benson, PhD, Assistant Professor of Strategy, Management
Hilary Hungerford, PhD, Associate Professor of Geography
Paul Monson, AIA, NCARB, Assistant Professor of Architecture

RESEARCH ASSISTANTS
Reese Boardman, Data Governance
Karissa Gillespie, Mail-in Ballot Study
Xander Greenwood, Utah Lake/Conservation
Josh Hadlock, Data Governance AI Developer
Jaxon Hill, Mail-in Ballot Study
Ethan Howlett, Data Governance AI Developer
Suzette Johnson, Mail-in Ballot Study
Avery LaGiglia, Mail-in Ballot Study
Keomony Mary, Synthetic Data Project
Christ Hermes Louyoko Nianza, Federalism Intergovernmental/ GIS Mapping
Bradley Smith, Data Governance
Dori Whitehead, Mail-in Ballot Study

EVENT ASSISTANTS
Emilee Cook
Jade Haymore
Elayna Saley

COMMUNICATIONS/GRAPHIC DESIGN ASSISTANTS
Catalina Aroca Baquero, Social Media
Katherine Brough, Graphic Design
Alexa Herrera, Communications
Kaitlyn Mayo, Graphic Design
Sophia Otis, Web Designer
Brooke Peterson, Graphic Design
Rebecca Whyte, Communications