PUBLIC POLICY BRIEF

Protecting the Right to Privacy in a Digital Era

Authored by James Czerniawski
Policy Analyst, Tech and Innovation

LIBERTAS INSTITUTE

SUMMARY

Private companies are constantly finding new and innovative ways of incorporating new technologies into their offerings. As they do, Americans are moving their lives into the digital realm.

While many of these products tout enhanced security protections for their consumers, the reality may be different than what they think.

Biometric technologies specialize in using identifying human features for verification of the user. From fingerprints to DNA to voice recognition, technology has opened up vast possibilities that were previously unimaginable.

While commercial uses of the technology can yield positive results, law enforcement is also using these tools to achieve their stated goal of protecting the community.

But the public is not always aware law enforcement is using these technologies in this fashion. There was no public buy-in, no discussion, and no process to establish guardrails to protect an individual's constitutionally protected rights.

The desire to use new technologies in the name of protecting the community cannot come at the expense of an individual's fundamental rights.

With the introduction of new technologies (both digital and not), an erosion of the Fourth Amendment began to slowly develop. Gathering information on people, once a long and strenuous endeavor, could be accomplished with mere computer keystrokes.[1]

The knowledge should come as no surprise—in fact, over 90% of all the data created in the world has been generated in the last two years alone. Every day, humans around the world generate over 465 exabytes of data, which is enough data to completely fill the storage capacity of nearly 589 million PlayStation 5 consoles.

More than ever, Americans are interfacing with the internet to perform many tasks they would normally have to do in person. Whether it's banking, shopping, researching, or employment, everyday life is becoming increasingly digital-centric.

The increasing interaction of individuals with these technologies often puts them in the crosshairs of law enforcement, who also use technology to assist them in a variety of matters. While previously, some things about people could easily be kept private due to the physical nature of interactions with the world, the internet does not abide by these constraints.

One clear example is biometric technology, which is used both by the government and private citizens. In 2013, Apple introduced the use of fingerprint recognition for the iPhone and iPad.[2] In 2017, the company made facial recognition available as an added security feature.[3]

Other companies have followed, implementing such features for broad consumer use and convenience. The government has long used fingerprints for identification purposes, and it sets the stage for conflict between citizens and law enforcement.

Rapid advances have also occurred in personalized DNA technology, where Ancestry.com[4] and 23andMe,[5] among others, have created privately-owned genealogical databases to allow for people to discover more about their family history. Some companies offer health guidance to customers based on their genetic profiles. Tens of millions of individuals have now provided their private DNA information to such companies.[6]

Society's adoption of technology and consent to its use has created gray areas in the law that overzealous law enforcement officers can take advantage of without placing a priority on the expectation of and right to privacy.

The legal principles regarding individuals' right to privacy do not evenly apply to digital devices.

If a law enforcement officer wants to obtain physical evidence, they must obtain a warrant to search private property for it. However, as material increasingly moves online, traditional Fourth Amendment protections are not being enforced. For example, law enforcement often does not need a warrant to access a person's data collected or stored by third parties. A simple subpoena, or even a direct request by an officer, can lead to the government gaining access to a person's private information.

This "third-party doctrine," as it is called, has long provided an exception to the warrant requirement for information about a person that is possessed by another. One form of this third-party data is cell site location information (CLSI), which is generated through pings off of cell towers and collected by third-party carriers like AT&T or Verizon, to track the location of connected devices.

The U.S. Supreme Court's recent ruling in Carpenter v. U.S. chipped away at this past precedent, holding that individuals do have an expectation of privacy in their cell phone location information, so now law enforcement now must obtain a warrant even though it is information held by a third-party provider.[7]

Utah's Legislature recently built upon the Carpenter case by passing House Bill 57 in 2019. The law requires state and local law enforcement to obtain a warrant in order to access a person's digital data, regardless of where it's stored or by whom.[8]

Additionally, the law also prohibits bulk data collection to ensure that the particularity requirement of the Fourth Amendment is enforced by statute when accessing large quantities of digital data about persons who might not be the suspect.[9]

It is this very requirement of particularity that presents a problem for law enforcement's access to digital data, specifically the exception provided by the plain view doctrine.[10] When searching a person's home, for example, law enforcement has the ability to search the property for evidence described in the warrant.

Should they see something in plain view not described in the warrant

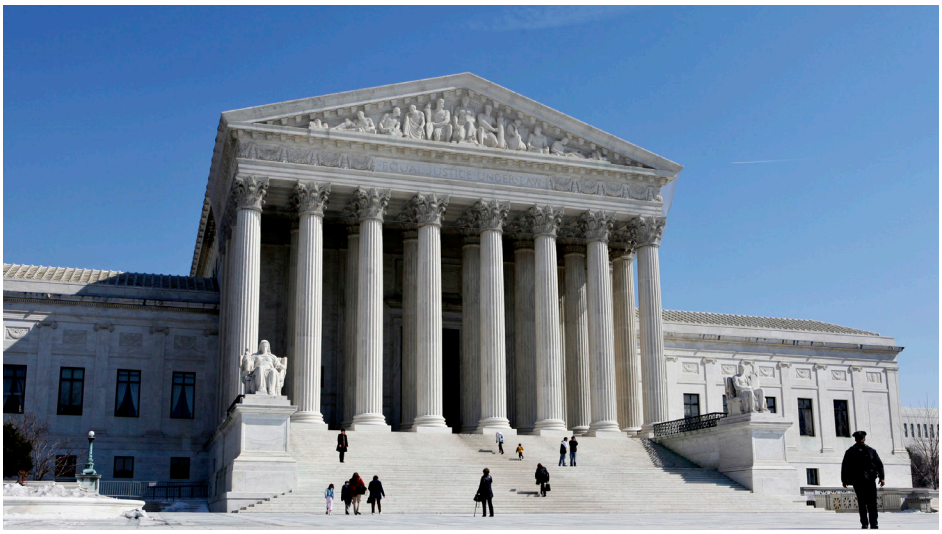
during the course of the search, and officers believe it is connected to the crime or separate evidence of criminal conduct, they can seize it and use the evidence to further charge the suspect. Of course, the plain view exception does not permit looking in areas of a home that are not allowed under the warrant.

These principles do not evenly apply to digital devices. When law enforcement seizes a phone, they can digitally clone the device, taking all information off the phone to search its contents for evidence of a crime. If looking for evidence of conducting drug sales, officers can look at information on banking apps, social media, photos, phone contacts, messages, and any other content on the phone.

This broad search—reviewing content that reveals intimate information about a person's entire life—places an alleged criminal in an extraordinarily compromising position. A person innocent of the alleged crime could have had their phone searched, only to find themselves in trouble for something completely different. The digital nature of data complicates the ability to particularize and narrow a search if officers have access to all contents of a device.

Technology & The Fifth Amendment

The Fifth Amendment of the Constitution is the crux of the relationship between an individual and their government, as it relates to criminal proceedings and due process. Particularly, the Fifth Amendment provides protections from double jeopardy, provides the right to a grand jury, requires the government compensate an individual if they forcefully take their property, and most importantly, provides protections from self incrimination.[11]



The U.S. Supreme Court has not kept up with technological advancements

The Fifth Amendment was included in the Constitution in response to the overreaching actions of the Courts of Star Chamber and High Commission—British courts that operated from 1487-1641.[12] Their judicial proceedings looked far different than anything the United States court system operates like.

Eventually, England disbanded these courts when switching to the common law system, which enshrined the notion of not being forced to self-incriminate. Even within the colonies, this tenet of the common law made its way into colonial founding documents and carried over into state constitutions.

The Fifth Amendment has also been complicated by new technological advancements. As one example, consider a locked cell phone seized by law enforcement pursuant to a warrant. If this device is locked, and law enforcement believes it contains evidence proving a suspect committed the crime, can the suspect be compelled to unlock their phone? Is it more permissible to compel the individual to biometrically unlock their phone, as with their fingerprint or facial scan, versus having them divulge or directly enter an alphanumeric passcode?

Courts have been inconsistent in determining the application of this constitutional protection to cases such as the above hypothetical. Part of the problem lies with the U.S. Supreme Court for not clarifying a difference between physical and mental communication and whether biometrics should be included under the Fifth Amendment.[13]

State courts have been relatively split on the issue of compelling an individual to unlock their devices for law enforcement. The Court of Appeals of Minnesota found that a court order issued to compel the defendant to unlock his cell phone did not violate the Fifth Amendment.[14]

In the case of *U.S. v Apple MacPro*, the U.S. Court of Appeals for the Third Circuit found that a judge may order an individual to provide unlocked un-encrypted devices if the device is proven to be owned by the defendant and is proven to contain evidence of the accusation.[15]

But in *Commonwealth v Bost*, a Virginia state judge ruled "law

enforcement may require a criminal defendant to provide his fingerprint—but not his passcode—to unlock a smartphone that might contain evidence that would be used against him at trial."[16]

Many of these cases were based on a concept used by law enforcement known as the Foregone Conclusion Doctrine.[17] The Forgone Conclusion Doctrine relies on three core principles. The state has to demonstrate that

1. It has knowledge of the evidence they are demanding;
2. The defendant possessed or controlled the evidence; and
3. The evidence is authentic.

Essentially, the government must show that the device in question contains evidence, that it is genuine, and that the evidence belongs to the accused.[18] Also, a layer of particularity has to be described by the government, so law enforcement cannot use generalized statements in their request from the court to acquire an order to compel.[19] However, this issue appears unsettled due to differing rulings from other judges. For example, a U.S. district court judge in Idaho denied law enforcement's request to obtain a search warrant that would allow them to compel the individual to use his or her fingerprint to unlock their cell phone.

The judge wrote that "compelling the use of the individual's fingerprints violates the fifth amendment rights against self-incrimination because the compelled unlocking of the phone with fingerprints would communicate ownership or control of the phone" and the search and seizure "would not be reasonable under the fourth amendment."[20]

The most recent case on this issue comes from the Supreme Court of Indiana, in *Seo v State*.[21]

In this case, the defendant called law enforcement to inform them she had been raped, and when they arrived, she allowed a detective to examine her phone for evidence. While the alleged rapist never had charges brought against him, the defendant was arrested and charged with felony stalking after detectives reviewed her text messages.[22] The court found that the Fifth Amendment protection against self-incrimination was applicable against a woman who refused to unlock her phone for law enforcement because complying with the order was a form of testimony under the Fifth Amendment.[23]

While law enforcement generally will argue that a warrant provides them the legal basis to compel biometric assistance of a suspect in gaining access to a digital device, the split nature of these rulings makes clear that this remains an unsettled legal question, and one for which new technologies have created urgency.

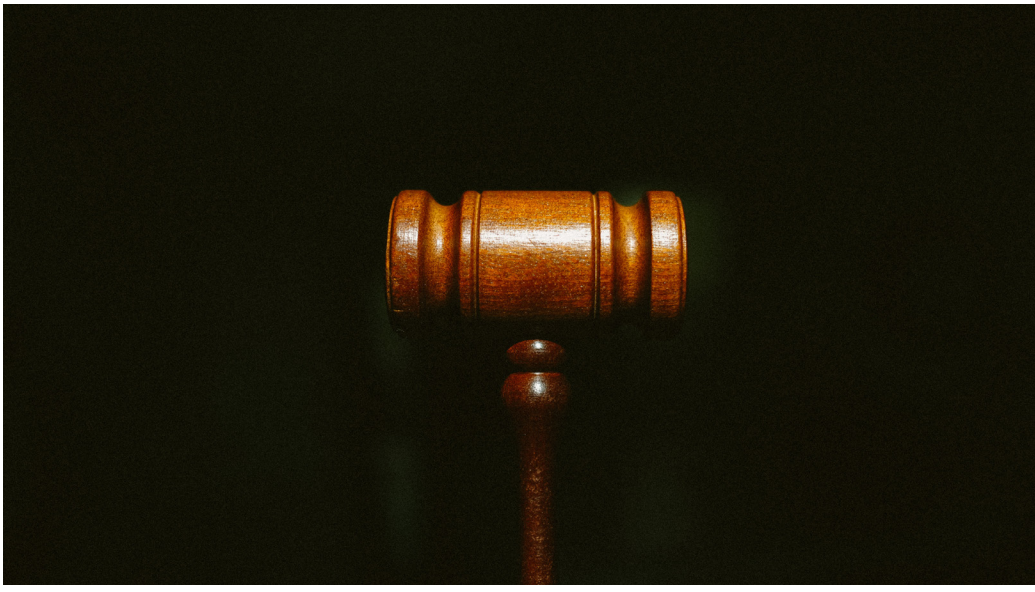
Problems with Biometrics and Mass Data Gathering

A: Existing Databases of Public and Private Information

The amount of data that is gathered on Americans in the age of the internet is unsurprising. Data is being generated incredibly fast, and that rate is only increasing. Law enforcement has tapped into this information for the purposes of investigations at one point or another.

Over 2.5 quintillion bytes of data are created by people every day.[24] Over 1 billion credit card transactions happen every day.[25] 57 million people in the United States use mobile banking apps on their phones.[26]

The healthcare system has produced databases filled with millions of people, the largest of which contains over 250 million patient records supporting 80 million patient visits each year.[27] A recent Gallup poll found 45% of Americans track their health via digital fitness trackers or mobile applications.[28]



Court rulings on data privacy have been mixed

Many Internet of Things (IoT) devices are implemented in daily life. In 2006, there were only about 2 billion such devices.[29] By 2025, the number of IoT devices could rise to as high as 41.6 billion.[30] This includes everything from voice controlled navigation systems to home security systems to smart wearables, like Fitbits, that people wear to track their health metrics.

Banjo, a Utah tech company, made headlines recently after it was revealed that it had obtained a contract worth $750,000 to build an intricate real-time surveillance system for the state's Attorney General's office.[31] The software boasted the ability to listen to 911 calls, scan social media posts, monitor traffic cameras, track the location of police cars, and more—providing quick and precise details of citizen conduct.[32]

As technology continues to evolve, it will open up more avenues and opportunities to leverage the technology in such a way that law enforcement can benefit from the information.

B: Facial Recognition Technology

In the 1960s, Woodrow Bledsoe developed a semi-automated facial recognition system to analyze facial features within an image.[33] 30 years later, the technology had progressed to the point of enabling real-time facial recognition.[34] While the technology offers many benefits, it's still fallible and imperfect. When used and heavily relied on by law enforcement, it can put innocent people, especially minorities, in the crosshairs of law enforcement.[35]

Robert Williams offers a cautionary tale of the consequences of over reliance on an incomplete technology. In January 2020, police in Detroit were looking for a suspect who robbed five watches from a store. When police received the security footage from the store, they ran it through their facial recognition software. The software gave them a name: Robert Williams, 42 years old in Farmington Hills, Michigan.[36]

This case is worth highlighting because it was one of the few times where police admitted that facial recognition technology was what prompted police to act and arrest Williams, in front of his wife and two children. When his wife asked what her husband was being arrested for, a law enforcement officer rudely replied, "Google it."[37] The footage from the security camera was grainy and low quality, and when Williams denied being the man in the photo, police retorted, "So I guess the computer got it wrong, too."[38]

Police relied so heavily on the technology that it became a detriment to the performance of their responsibilities. They detained Williams for 30 hours, then released him on bail until a court hearing could be set for his case. They never bothered asking about Williams' whereabouts that day. There was not even a witness to the crime.[39]

New technologies can be a powerful tool, but when used incorrectly, the costs to innocent individuals can be exorbitantly high.

Ultimately, the prosecutor in Wayne County dropped the charges against Williams, citing insufficient evidence.[40] Williams was taken away from his family, forced to sit in jail for 30 hours, and had to make bail. He was treated as a criminal as a direct result of improper use of facial recognition technology, all for a crime he did not even commit.

Consider the example of the Amazon Ring Doorbell. One of the most popular smart locks on the market, the lock includes a camera feature so homeowners can see who is at their door. With the ever-increasing number of homes installing such locks, it is unsurprising to see that law enforcement wants a piece of the action.

Amazon is more than happy to assist in this regard. In fact, Amazon has actively engaged in partnerships with law enforcement, having over 1,400 agreements with local law enforcement agencies.[41]

Situations like these reinforce why it is important to proactively address technology policy issues as opposed to waiting for courts to do so, potentially years or even decades after they are first utilized by government actors. New technologies can be a powerful tool, but when used incorrectly, the costs to innocent individuals can be exorbitantly high. A framework needs to be established where the harm to individuals can be mitigated sufficiently.

C: Voice Recognition

According to Steven Cooper, Barclays' head of personal banking, "Unlike a password, each person's voice is as unique as a fingerprint."[42] It is unsurprising that voice recognition technology has developed over

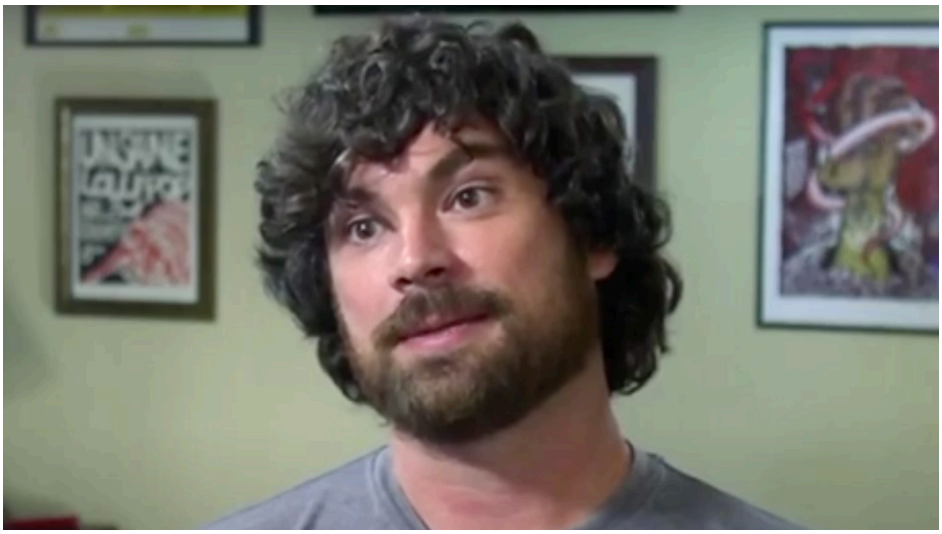
the years to recognize speech for different purposes. The technology made massive strides, with voice recognition technology being used in the workplace by the 1990s.

Today, voice recognition technology is used as a method of improving daily life. Take Siri, Apple's virtual assistant. It has numerous of features, from comprehending complete sentences to checking the weather, sending messages to contacts, making phone calls, and more.[43] Cars integrate voice commands to make phone calls, set GPS destinations for travel, and more.

Unsurprisingly, the technology has found its way into use by law enforcement. While it can be used for consumer purposes, like the aforementioned improvements, law enforcement can use it to assist them in identifying the voices of people they are surveilling.

Verification plays an important role in investigations, and people are not the best resource to rely on in those instances. While people can accurately identify familiar voices, they struggle to identify unfamiliar voices in ear witness testimony, making them unreliable and inaccurate.[44] Current voice recognition technology can scan about 10,000 voices every five seconds and can identify someone 90% of the time when the audio clip is at least 15 seconds long and good quality.[45]

This technology can easily be integrated into existing ones. Let's return to the example of the Amazon Ring Doorbell.[46] These systems have the ability for consumers to interact with people who arrive at their door by speaking through their related products.[47] This means that if that video/audio footage were shared with law enforcement, they could harvest the voices of dozens of innocent people who interact with another person's private home.



Michael Usry, Jr. was arrested for murder because his father shared his own DNA

Like any novel technology, in order to be reliable, law enforcement would need to have access to an inordinate amount of data. While Rosalynn Carter once said, "There is nothing more important than a good, safe, and secure home,"[48] it can not come at the expense of a person's reasonable expectation of privacy.

D: DNA Databases

Michael Usry, Jr.'s father submitted DNA through a project sponsored by The Church of Jesus Christ of Latter-day Saints as a public database. The project and database were eventually acquired by Ancenstry.com, one of the leading for-profit firms in genealogy.

The company received a court order to reveal the last name of a DNA sample's owner to police, which was contained in this database. Detectives used the information to persuade a judge in Louisiana to sign off on a search warrant for Usry, Jr. to provide his DNA to compare it against that of the sample they suspected belonged to a person who had committed rape and murder in 1996.[49]

This tactic of "genetic genealogy," using DNA information and private databases as a source to build leads and identify unknown samples, is becoming increasingly common—but they are often inaccurate. One study conducted in 2014 found only 17% of familial genetic searches led to the identification of a relative to the true offender.[50] That is an astoundingly low level of success, meaning that a large number of innocent people are being incorrectly targeted as a result of these types of searches.

These "fishing expeditions" into massive databases to generate leads often present more problems than solutions for cases. The process inherently violates an individual's

reasonable expectation of privacy and their consent for providing such DNA samples to begin with.

Given the shared nature of DNA information, the question about consent becomes even murkier since relatives can expose close family members and distant cousins alike without their knowledge or permission. Such broad searches seem to violate the particularity requirement of the Fourth Amendment.

Fortunately for Usry, he was cleared from being a suspect in the murder case. This came after his initial arrest and weeks of being accused by law enforcement of a murder he did not commit. But Usry's life was interrupted and profoundly impacted because law enforcement used a new technology in a way that allowed them to disrupt an innocent person's life.[51]

What Needs to Happen

Part of the underlying issue when it comes to law enforcement utilizing technology is the nature of the data they are trying to access. While publicly available information on people is well within law enforcement's rights to tap into, when it comes to data being produced for private use, the lines become blurred.

The responsibility of thinking about the implications of law enforcement's use of technology falls not just on law enforcement agencies, but on businesses too. Technology companies must consider how the tools they design and sell to police departments minimize accountability and exacerbate injustice.

It is imperative to scrutinize how the products they design could alter the relationship between the government and individuals. Companies should not be in the business of profiting by exploiting irrational fears of crime.

As individuals increasingly incorporate digital technology into their everyday lives, the collision course between themselves and law enforcement accelerates. Automation, artificial intelligence, facial recognition, digitalization of information, and the proliferation of biometric security have placed the criminal justice system in a radically different position than it was just three decades ago.

Individuals' relationship with government has fundamentally changed because of technological advancements and the power it places in the hands of the state.

Government's access to personal information is governed by the warrant process. But is judicial review adequate to the task? Part of the issue is the fact that jurisprudence has a hard time keeping up with technology. This is due to Martec's Law, which states that technology grows exponentially while the government's ability to adapt and regulate is more logarithmic in nature.

These "fishing expeditions" into massive databases to generate leads often present more problems than solutions for cases.

New technologies, such as biometric access to a device, are unrolled at breakneck speed. Law enforcement tends to avail themselves of such tools as they become available. Only later are restrictions enacted when their use is challenged in court. But this delayed protection is inadequate.

Courts disagree when it comes to the application of new technologies to existing precedent. The inconsistency in rulings on biometric access highlights how new technologies can fundamentally alter previously held notions of appropriate levels of government intrusion into privacy. It will be some time until the Supreme Court is able to clarify its previous opinion dealing with alphanumeric locks on devices and its application to new biometric features.

But such a ruling should not end the discussion, since it was the Court that created the "third-party doctrine" that now permits most law enforcement agencies to access people's private information without a warrant. More protections, proactively put into state law, are needed beyond the delayed constitutional floor established by the Court.

As Justice Samuel Alito once wrote, "[Courts] are very ill-positioned to make these determinations…. We are not up on all the latest technology. If privacy is to be protected in the future… state legislatures should take the lead."[52]

First, there must be limits imposed on the kinds of data that law enforcement has access to when accessing or cloning a suspect's device; the particularity requirement of the Fourth

Amendment must hold true when accessing a person's entire digital existence. In reality, not all digital data is evidence, but simply digital information considered private by someone who has a reasonable expectation for that to be respected.

That expectation should extend into the courtroom, as well. Law enforcement needs to articulate with specificity the evidence they are looking for on a device and where it could be found. It is unacceptable that a person could be potentially culpable for completely unrelated crimes simply because the plain sight doctrine could not be evenly applied when collecting evidence from an electronic device.

New technologies must be vetted transparently and proactively before being used by law enforcement and government agencies. Having a dedicated office or committee review these technologies and solicit public involvement will facilitate a conversation that prevents the secret or opaque use of new tools without public knowledge or consent.[53]

Such guardrails will ensure that people's right to privacy is better protected and help deter what some fear is becoming an Orwellian surveillance state.

Policymakers also need to directly confront the question of biometric access and set boundaries around when law enforcement agents can compel access to a person's locked device. Split court rulings show the unsettled nature of this question, and it may be years before the U.S. Supreme Court takes up the issue, if it does at all.

New technologies bring new twists to previously settled legal questions.

But as Justice Alito articulated, state legislatures are better positioned to respond to policy questions such as this. Elected officials should therefore establish a set of limits within which such compulsion can be permitted for egregious conduct and exigent circumstances and prohibit it for all other cases so as not to force people to reveal their personal information and therefore incriminate themselves.

Lastly, there needs to be independent, credible, and consistent auditing of technologies being used by the government. These independent audits should be made available to the public for general consumption. Developing a framework for establishing an audit process is crucial. Audits are a unique mechanism that can establish a semblance of credibility that actors are abiding by any guardrails set in place.

Law enforcement officials need to investigate crime and collect evidence for prosecutors to use in order to uphold the law. Technology has increasingly become part of this process, and rightly so. But without proactive restrictions and limits put in place by policymakers, the balance between privacy and security swings too far in favor of the state, with courts unable to keep up.

New technologies bring new twists to previously settled legal questions, and their rapid development makes matters worse. While many defer to the courts to resolve such questions, law enforcement agencies continue to acquire and utilize new tools and technologies that facilitate their job while potentially undermining the rights and privacy of those they are tasked to serve.

By establishing a process that places proactive limits on these technologies, a better balance can be struck between protecting these rights while simultaneously enabling law enforcement officers to reasonably achieve their goals.

PROPOSAL A: THE PRIVACY PROTECTION ACT

In the pursuit of protecting Utahn's privacy rights, the Utah Legislature should consider passing our landmark proposal, The Privacy Protection Act.[54] The legislation would:

- Create and fund a State Privacy Officer within the State Auditor's office. The officer would be appointed by the Auditor.
- The Auditor will assemble a Personal Privacy Oversight Committee, composed of 7-8 volunteer tech/privacy experts/advocates, along with 1-2 law enforcement representatives. This will be done on an ad-hoc basis for the short term by the Auditor. This should be formalized in statute later, to give the committee oversight authority and legitimacy to ensure government agencies/entities respond.

- States that a government agency/entity may not use a technology/software/process that the Personal Privacy Oversight Committee has recommended against using unless the relevant legislative body enacts a law specifically authorizing its use.
  - ◊ For state agencies/entities, the use must terminate by May 1 unless specifically authorized by the Utah Legislature.
  - ◊ For local governments, the use must terminate within 60 days unless specifically authorized by the county or city council.
- Each favorable recommendation of a technology/software/process by the Committee shall sunset within two years, at which point the State Privacy Officer shall perform a review to determine if anything has changed about the use of the technology/software/process (additional data being used, more expansive use, etc.). If so, the Committee shall flag it for committee review and analysis.
- In 2021: the Officer and Committee shall focus on topics surrounding:
  - ◊ Use of video and audio feeds for synthesis/analysis to facilitate surveillance (past or present) by law enforcement using:
    - * public sources (911 calls, traffic cameras, body cameras, drones, etc.)
    - * private sources (CCTV, doorbell cameras, etc.)
  - ◊ Bulk analysis of social media feeds to recommend action/intervention by law enforcement.
  - ◊ Use of biometrics by law enforcement
    - * Compelling a person to provide access to their entire digital life via a facial or fingerprint scan.
    - * Facial recognition technology, both using government databases and social media photos of people.
    - * Using public/private DNA databases to search for the identity of unknown people.
  - ◊ Review data-sharing agreements among state agencies with third party participants, including but not limited to: federal agencies, private entities, nonprofit organizations, and public colleges and universities.
- In 2021, the Officer will present to an interim committee to offer recommendations to the legislator to consider for the 2022 session.

The goal should be to pass a robust and comprehensive omnibus privacy reform bill that enacts necessary reforms, restricting government use of private information to better protect privacy and ensure information is used consistent with the purposes for which it was created (so as to prevent “scope creep” and surveillance where it was never expected or authorized.

PROPOSAL B: A MORATORIUM OF EARLY ADOPTION OF TECHNOLOGY BY PUBLIC ENTITIES

A more stringent approach would be to place a moratorium on the use of new, emerging, or morally and ethically shaky technologies by government agencies in the process of carrying out their duties.

The reality is that new and emerging technologies are exactly that — new. They have not worked out the various issues they currently possess, and it would be ludicrous to enable a public entity to leverage an unproven and flawed technology for an “ends justify the means” theory. Other technologies, like genealogical databases, raise serious moral and ethical concerns over consent and the extent of information they can provide. Warrants, while normally viewed as a safeguard, are proving to be increasingly more like rubber stamps. Courts need support in understanding the technologies they are approving warrants of using, so they can better understand the nature of what they are signing off on. Only when sufficient progress has been made with technology and sufficient guardrails have been put in place should a publicly funded entity be able to use such technologies.

Endnotes

1. Libertas Institute Staff. *Protecting Your Digital Data From Warrantless Searches*. February 7th, 2019. https://libertasutah.org/policy-papers/digital_privacy.pdf.
2. Apple Staff. "Apple Announces iPhone 5s—The Most Forward-Thinking Smartphone in the World." Apple Press Release. September 10, 2013. https://tinyurl.com/apple-fingerprint.
3. Clare Garvie and Michel Martin. "Apple Gets Mixed Reactions To New iPhone's Facial Recognition Technology." *NPR's All Things Considered*. September 17, 2017. https://tinyurl.com/npr-apple.
4. "AncectryHealth." Accessed December 20, 2020. https://www.ancestry.com/health.
5. "23andme." Accessed December 20, 20202. https://www.23andme.com/?mkpc=true.
6. Antonio Regalado. "More than 26 million people have taken an at-home ancestry test." *MIT Technology Review*. February 11, 2019. https://tinyurl.com/ydbwczzo.
7. *Carpenter v. United States*. No. 16–402. Argued November 29, 2017—Decided June 22, 2018. https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.
8. Utah H.B. 57. Signed to law March 27, 2019. https://le.utah.gov/~2019/bills/static/HB0057.html.
9. Ibid.
10. "Plain View Doctrine." Legal Information Institute, Cornell Law School. Accessed July 19, 2020. https://www.law.cornell.edu/wex/plain_view_doctrine.
11. "Fifth Amendment." Legal Information Institute, Cornell Law School. Accessed November 4, 2020. https://www.law.cornell.edu/constitution/fifth_amendment.
12. Dalia Lithwick. "Where Did the Fifth Amendment Come From?" Slate. February 12, 2002. https://tinyurl.com/y8szjmcd.
13. *Commonwealth of Pennsylvania v. Joseph J. Davis*. No. 56 MAP 2018. Argued May 14, 2019—Decided November 20, 2019. https://tinyurl.com/yaudmosp.
14. *State of Minnesota v. Matthew Vaughn Diamond*. No. 10-CR-14-1286. Filed January 17, 2017. https://tinyurl.com/y7l2sjya.
15. *United States of America v. Apple Macbook Pro Computer Apple Mac Mini Computer Apple Phone Plus Cellular Telephone Western Digital My Book For Mac External Hard Drive*. No. 15-3537. Decided March 20, 2017. https://caselaw.findlaw.com/us-3rd-circuit/1853477.html.
16. "Criminal Defendent Required to Provide Smartphone Fingerprint, but Not Passcode." The National Law Forum. November 5, 2014. https://nationallawforum.com/tag/commonwealth-v-baust/.
17. Zak Goldstein. "Foregone Conclusion Doctrine Allows Government to Make Criminal Defended Disclose Computer Password." Goldstein Mehta, LLC. December 2, 2017. https://goldsteinmehta.com/blog/foregone-conclusion-doctrine.
18. Ibid.
19. Ibid.
20. "Idaho Judge Denies Search Warrant Asking for Forced Fingerprint Unlock of Google Pixel." United States District Court for the State of Idaho. Case No. 1:19-mj-10441-REB. Filed May 8, 2019. https://tinyurl.com/yc3za4ho.
21. Andrew Crocker. "Victory: Indiana Supreme Court Rules that Police Can't Force Smartphone User to Unlock Her Phone." Electronic Frontier Foundation. June 23, 2020. https://tinyurl.com/yc4983sx.
22. Ibid.
23. Ibid.
24. Michael Einstein. "Some Amazing Statistics about Online Data Creation and Growth Rates." Information Overload Research Group. April 17, 2019. https://iorgforum.org/case-study/some-amazing-statistics-about-online-data-creation-and-growth-rates/.
25. Staff. "How America Banks: Household Use of Banking and Financial Services." Federal Deposit Insurance Corporation. Updated October 19, 2020. https://tinyurl.com/ybtaclcp.
26. M. Szmigiera. "Mobile banking in the U.S.- Statistics & Facts." Statistica. October 8, 2019. https://www.statista.com/topics/2614/mobile-banking/.
27. Staff. "Cerner CEO: Data Will Drive Global Health Care Transformation." Cerner. October 13, 2020. https://tinyurl.com/yae6jv53.
28. Justin McCarthy. "One in Five U.S. Adults Use Health Apps, Wearable Trackers." Gallup. December 11, 2019. https://news.gallup.com/poll/269096/one-five-adults-health-apps-wearable-trackers.aspx
29. Ibid.
30. IDC Staff. "The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast." International Data Corporation. June 18, 2019. https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

Endnotes - Continued

31. Leia Larsen. "Utah Company Banjo Is Building a Massive Surveillance System with the Help of the State's Attorney General." *Salt Lake Tribune*. March 8, 2020. https://www.sltrib.com/news/politics/2020/03/08/utah-company-is-building/.
32. Ibid.
33. Jeremy Norman. "Woodrow Bledsoe Originates of Automated Facial Recognition." Jeremy Norman's History of Information. Updated December 30, 2020. http://www.historyofinformation.com/detail.php?entryid=2495.
34. Matthew A. Turk and Alex P. Pentland. "Face Recognition Using Eigenfaces." Massachusetts Institute of Technology. 1991. http://www.cs.ucsb.edu/~mturk/Papers/mturk-CVPR91.pdf.
35. Drew Harwell. "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use." *Washington Post*. December 19, 2019. https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.
36. Bobby Allyn. "'The Computer Got It Wrong': How Facial Recognition Led To False Arrest of Black Man." NPR. June 24, 2020. https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig.
37. Ibid.
38. Ibid.
39. Ibid.
40. Ibid.
41. Jason Kelley and Matthew Guariglia. "Amazon Ring Must End Its Dangerous Partnerships With Police." Electronic Frontier Foundation. June 10, 2020. https://www.eff.org/deeplinks/2020/06/amazon-ring-must-end-its-dangerous-partnerships-police.
42. Hugh McLachlan. "Is every human voice and fingerprint really unique?" The Conversation. August 11, 2016. https://theconversation.com/is-every-human-voice-and-fingerprint-really-unique-63739.
43. Peter Economy. "25 Surprisingly Useful Things You Can Do With Siri." *Inc*. January 9, 2019. https://www.inc.com/peter-economy/25-surprisingly-useful-things-you-can-do-with-siri.html.
44. Carolyn McGettigan and Nadine Lavan. "Human Voices Are Unique but We're Not That Good at Recognizing Them." *Scientific American*. June 19, 2017. https://www.scientificamerican.com/article/human-voices-are-unique-but-were-not-that-good-at-recognizing-them/.
45. Staff. "How Is Speech Recognition Used in Law Enforecement?" Dictation Store. Accessed December 20, 2020. https://www.dictation-store.com/speech-recognition-law-enforcement-s/239.htm
46. "Ring." Amazon. Accessed December 20, 2020. https://www.amazon.com/dp/B08N5NQ869/.
47. Ring. "Ring Activation." Amazon. Accessed December 20, 2020. https://tinyurl.com/y9fllf43.
48. Rosalynn Carter. "Rosalynn Carter Quotes." Brainy Quote. Accessed December 20, 2020. https://www.brainyquote.com/quotes/rosalynn_carter_392323.
49. William Brangham, Nsikan Akpan, and Rhana Natour. "A father took an at-home DNA test. His son was then falsely accused of murder." PBS News Hour. November 7, 2019. https://www.pbs.org/newshour/show/a-father-took-an-at-home-dna-test-his-son-was-falsely-accused-of-murder.
50. C.N. Maguire, L.A. McCallum, C. Storey, and J.P. Whitaker. "Familial searching: A specialist forensic DNA profiling service utilising the National DNA Database® to identify unknown offenders via their relatives—The UK experience." *Forensic Science International: Genetics*, vol. 8, no. 1. January 2014. Pages 1-9. https://www.sciencedirect.com/science/article/abs/pii/S1872497313001543.
51. Kyle Swenson. "Police twice targeted the wrong men for a brutal 1996 killing. A cigarette butt changed everything." *Washington Post*. May 17, 2019. https://www.washingtonpost.com/nation/2019/05/17/police-twice-targeted-wrong-men-brutal-killing-cigarette-butt-changed-everything/.
52. "Justice Alito: Legislatures Must Pass 21st Century Privacy Laws, Can't Be Left to Courts." Privacy SOS. September 21, 2020. https://privacysos.org/blog/justice-alito-legislatures-must-pass-21st-century-privacy-laws-cant-be-left-to-courts/.
53. For example, it was a surprise to elected officials and the public at large in late 2019 when a journalist revealed that the Utah Department of Public Safety had been using facial recognition technology for nearly a decade, using people's driver license photos, including those of minors, to be scanned several times daily.
54. Libertas Institute Staff. "Proposal: The Privacy Protection Act." Libertas Institute. May 14, 2020. https://libertasutah.org/limited-and-open-government/proposal-the-privacy-protection-act/.

PUBLIC POLICY BRIEF

Protecting the Right to Privacy in the Digital Age

LIBERTAS INSTITUTE

FREQUENT RECURRENCE TO FUNDAMENTAL PRINCIPLES IS ESSENTIAL TO THE SECURITY OF INDIVIDUAL RIGHTS

UTAH CONSTITUTION
ARTICLE I, SEC 27

2183 West Main Street, Suite A102, Lehi UT 84043 | 801.901.0310 | LibertasUtah.org