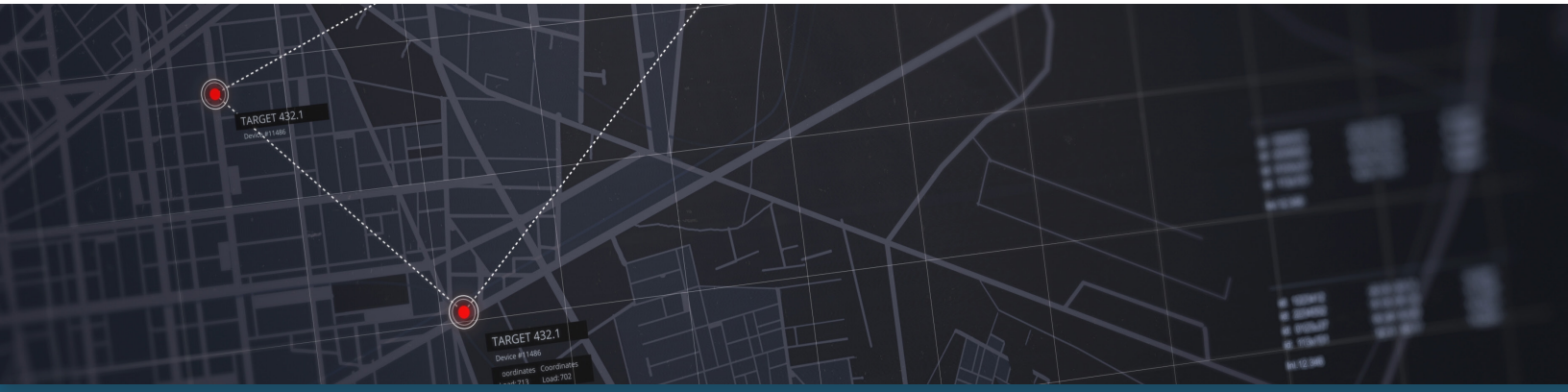
PUBLIC POLICY BRIEF

Securing States and Individuals from Surveillance

LIBERTAS INSTITUTE



SUMMARY

It's no secret that consumer data is collected by various private companies. Google, Instagram, and others routinely collect information about our locations, preferences, and habits. The databases that store this information are a valuable resource with many applications.

But private companies and consumers are not the only entities interested in leveraging this information. Governments have an interest in obtaining this data fulfill various government policy goals.

One example are reports that document social media companies collaborating with the U.S. government to craft policies and censor information. Government entities work with these companies to advance administrative goals.

This is one of many examples of a broader trend. Across all governmental sectors, state actors seek to either compel corporate entities to provide consumer information to the government or agents contract with companies whose main function is to utilize highly invasive technologies to serve government functions.

As technology continues to advance, states must place limits on collaborative relationships between corporate entities and government agents.

Banjo: A Cautionary Tale

Utah is not immune from efforts to merge corporate and state power. The now infamous Banjo controversy is a cautionary tale of what could have occurred in our own backyard. Banjo promised to work as an "event detection engine" for law enforcement.[1] In practice, this meant the company would use artificial intelligence (AI) technology to scan real-time public information from a variety of sources, including traffic cameras, social media, weather data, 911 calls, and weather data.[2]

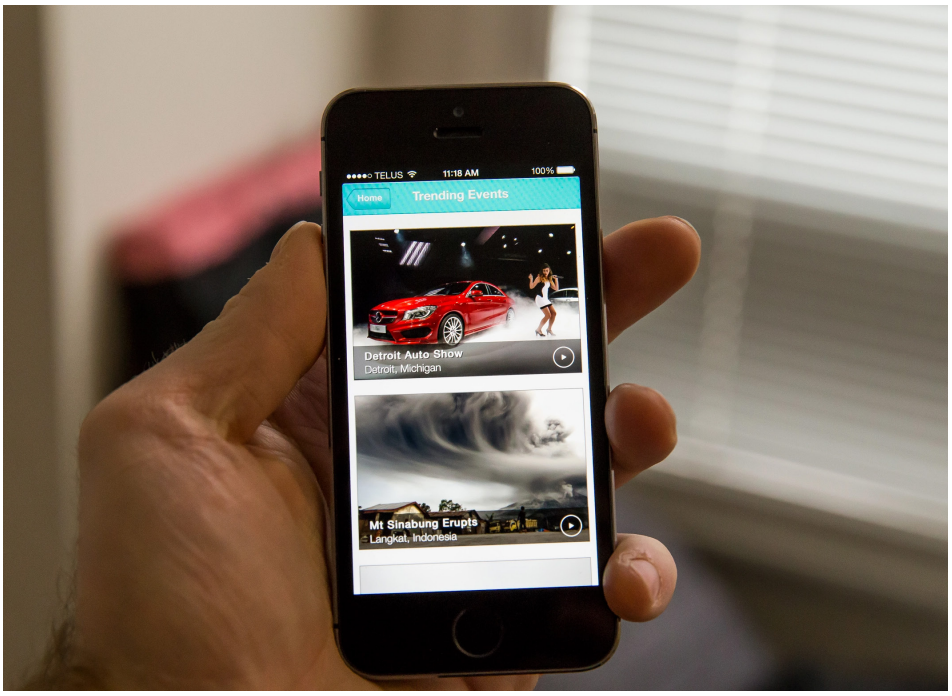
The AI algorithm then synthesizes this information to provide information to law enforcement agents.[3] Banjo never delivered on these promises.

Although the attorney general's contract with Banjo was canceled when the founder's ties to the KKK were revealed, the underlying premise of the contract was not rejected.[4]

Privacy problems and the potential for state abuse of power were not related to the canceling of contracts. Indeed, before the deal fell through, Attorney General Sean Reyes expressed enthusiasm at the idea of law enforcement having access to "un-siloed information" at "hyperspeed."[5]

The Rise of Surveillance Cities

China's surveillance system relies on centrally linked databases that include numerous data points related to human behavior.[6] Facial recognition, fingerprints, travel history, and footage from cameras mounted throughout cities are analyzed by AI software to keep the machine of government surveillance running.



By analyzing large swaths of behavioral data, the Chinese government hopes to perfect predictive policing and create the conditions for social stability.[7] Security, not freedom, is what the government seeks to achieve.[8]

Surveillance State: Inside China's Quest to Launch a New Era of Social Control, a new book written by Wall Street Journal reporters John Chin and Liza Lin, details the Communist nation's use of technology to surveil the public.[9] In the mind of China's leading e-commerce company, Alibaba, data drives the future.

Utah is not immune from efforts to merge corporate and state power. The now infamous Banjo controvery is a cautionary tale of what could have occurred in our own backyard.

Jack Ma, Alibaba's CEO is convinced that "[w]hoever owns enough data and computing ability can predict problems, predict the future, and judge the future."[10]

Whether this bold claim is true or not may be up for debate, but the use of technology necessary for centralized social control is powerful and not limited to China's totalitarian government.

Across the sea, in the land of the "free," American cities grapple with how to use — or ban — the government's use of personally invasive technology.

San Francisco serves as a case study in surveillance policy. It is a highly progressive city, but one that is unsure of how to solve problems that come with a spike in violent crimes.

In May 2019, the city became the first in the nation to ban law enforcement's use of facial recognition technology.[11] Fast forward to 2022 and conditions in the city have deteriorated. Post-pandemic, the city is dealing with a crisis of crime. San Francisco Mayor London Breed describes the problem in stark terms, stating the city is compassionate but must "draw the line with those who choose violence and a life of crime."[12]

This description comes at the beginning of the mayor's Medium post, an article designed to sell an unsure public on the benefits of a controversial city proposal that would allow law enforcement to access live footage from the city's private companies.

Breed described the ban on police use of live video in circumstances that do not involve imminent danger as removing necessary tools from the hands of law enforcement. This, she argues, leaves the public vulnerable.

Statistically, the rise in crime is complicated. Some crime has decreased in the city since 2019, but there has been a rise in violent offenses, including homicides, shootings, and car theft.

According to researchers, "Increases in crime could very well be temporary, therefore ratcheting up the surveillance apparatus in U.S. cities is unnecessary."

The political mood in the city shifted this summer with the ousting of the progressive district attorney, Chesa Boudin, who was perceived as being too lenient on crime. As the political winds shift, so have Breed's policy positions. She is proposing legislation to amend the city's Administrative Code.

San Francisco serves as a case study in surveillance policy. It is a highly progressive city, but one that is not sure how to solve problems that come with a spike in violent crimes.

This change would allow police to access the cameras and surveillance networks "owned, leased, or operated" by private businesses. If approved, the law would allow live monitoring of video activity for the purpose of gathering evidence and investigating open cases. Unfortunately, San Francisco is not alone in its quest to access data from businesses. In 2020, the San Diego Union Tribune reported that a city initiative from several years prior paved the way for widespread police surveillance.

San Diego installed new high-tech LED cameras. This was billed to the public as a way to gain better knowledge of mobility in the city. If the movement of people and cars was tracked, perhaps traffic in the future could be eased. The implementation of this plan involved the installation of cameras on more than three thousand city streetlights.

Skeptics of the system feared the creation of a surveillance network. Their fears were confirmed when it became public knowledge that police could access footage from the newly installed network of cameras.

The San Diego City Council has since shut down the program and passed an ordinance barring the use of technologies that can monitor and identify individuals without the approval of the city council.

West Coast cities are not the only ones struggling with decisions regarding the widespread use of surveillance systems.

In February 2022, Houston announced the implementation of the One Safe Houston plan, a blueprint to guide the city out of what Mayor Sylvester Turner described as a "public health crisis" brought on by a rise in violent crime.

Mayor Turner's plan to ensure safety in his city includes the implementation of a draconian new law requiring certain businesses to install surveillance cameras and turn over footage to law enforcement. The new mandate requires night clubs, convenience stores, and bars to install surveillance cameras.

Businesses must keep the data from these cameras for at least thirty days and turn over the footage to law enforcement within three days of the commission of a crime.

Current Law Reinforces Perverse Incentives

The rise of surveillance cities is made possible by the practical realities of technological advancement paired with the current legal landscape. Technological advances in facial recognition and AI software now make surveillance at scale feasible.

Two legal doctrines make it difficult to establish liability for actions that violate constitutional values and principles. These are the third-party and state-action doctrines.

For geofence warrants, government agents draw a virtual boundary around a crime scene and request all user data within this boundary during a spexific time period from tech companies, like Google and Verizon.

The third-party doctrine states that any information an individual shares with others, even information otherwise considered confidential, like banking records, loses constitutional protection covered by the Fourth Amendment.

The doctrine of state-action attaches liability to actions taken by private entities that "may be fairly treated as that of the State itself."

However, the tests that courts apply to determine whether a violation of state action has occurred are confusing, contradictory, and controversial.

Because of the high burden of proof imposed on plaintiffs before establishing liability, the doctrine does little to dissuade government entities and corporations from engaging in highly collaborative relationships.

Because it is hard to establish constitutional liability, it is easy for the government to delegate responsibilities to private companies through contractual relationships, thus avoiding the harsh scrutiny they would otherwise face.

These contractual relationships exist across numerous industries, from prisons, to schools, to military contracting. The end result is that public and private functions become increasingly interconnected.

The third-party doctrine paired with the difficulty of establishing state action has created fertile ground for the government to delegate responsibilities to private companies through contractual relationships, thus avoiding constitutional scrutiny and liability.

Geofence Searches Monitor Individual Movement

Geofence searches are a type of reverse search warrant used by law enforcement across the nation and in the state of Utah. Police increasingly rely on these broad "warrants" when investigating crime.

Agents draw a virtual boundary around a crime scene and request all user data within this boundary during a specific time period from technology companies, like Verizon and Google.

To address the vast number of incoming requests from law enforcement, Google took it upon themselves to establish a three-step process when turning over information to law enforcement. Initially, Google provides anonymized user data within the geofence during

the time specified by the police in their warrant.

After reviewing this cache of data, agents may request more information from Google. The end result of this process involves an unmasking process where police obtain the identity of a possible suspect who may have committed the crime under investigation.

This process violates the Fourth Amendment by skirting the particularity requirement. Instead of requesting information regarding a specific individual suspected of committing a crime, law enforcement agents utilize the warrant process to go on a fishing expedition in search of a suspect.

However, despite the constitutional defects, these searches are used across the nation. Due to the slow speed at which the judicial system moves, it is unclear if and when this investigative technique will go under the microscope of the judicial process.

Although a judge in Virginia recently ruled that a geofence search failed to meet Fourth Amendment requirements, her ruling was narrow and has limited jurisdictional applicability.

Functionally speaking, Google is still engaging in evidence gathering on behalf of law enforcement agencies in the state of Utah, meaning the state has essentially transformed corporate resources from private to public use.

Given the current state of judicial doctrines, the incentives encourage police to continue seeking data from corporations. Geofence searches

are only the tip of the iceberg in Pandora's box of reverse search "warrants." This year, the first lawsuit was filed challenging how police obtained a defendant's Google search history.

Practically speaking, absent legislative action, location and search history will not be the only data points mined by government agents using the process of reverse search warrants. Vast databases of information are already on the internet, including data uploaded by users who were unable to anticipate the future consequences of their actions.

For example, consumers who uploaded images to Facebook, Instagram, Flickr, or other popular websites were not thinking of the possibility that years later, sophisticated facial recognition software could crawl the web to collect this data without their consent.

Furthermore, the incentive structure that encourages businesses like Banjo to market their surveillance services to government agencies continues to exist. It is only a matter of time before more jurisdictions across the United States — including Utah — will be forced to confront the problem posed by the ease with which governments can surveil the public.

The rapid rate with which technology is moving coupled with the ease in which government actors can obtain privately-collected data threatens to undermine the consent of the governed. In the current climate, it would be a mistake for legislators to hope judicial responses are sufficient to address these issues.

Instead, Utah should follow the sage advice of Justice Alito, who trusts the legislative branch to tackle these issues. It is the people's branch who is best situated to "balance privacy and public safety in a comprehensive way."

Policy Recommendations to Protect Utahns' Privacy

To prevent the Orwellian scenes playing out in cities such as Houston and San Francisco, Utah should pass reasonable reforms to protect the public from the privacy dangers posed by widespread police surveillance.

The state legislature should undercut the porous relationship between businesses with large consumer databases and government agencies by restricting the government's ability to easily access information collected by private companies.

- Utah should pass a law barring police from conducting broad geofence searches that implicate innocent people unnecessarily. Codification of this Fourth Amendment standard would ensure Utahns are not subject to unreasonable searches and seizures by ensuring that new technological tools such as this are subject to the same constitutional protections. Short of a total ban on this practice, the following minimum standards should apply:
    - » A warrant should be required with notification to the judge that this type of request, if authorized, will inevitably include innocent people who were at a particular location but were not involved in the commission of any crime.
    - » Individuals whose location is unmasked as a result of a geofence warrant should be notified by law enforcement that they were the targets of such an operation.
    - » Any data obtained by law enforcement regarding innocent people, resulting from a geofence warrant, should be promptly and permanently deleted.
    - » Law enforcement should be prohibited from doing bulk data analysis of location data to ensure that the "anonymous" data they first receive from telecom providers is not de-anonymized through comparison with other data sets.
    - » Annual reporting to the Legislature regarding the use of geofence warrants to better shape future policy.

- The legislature should bar law enforcement from using video for real-time, 24/7 surveillance of public places. This would mean the use of telephone pole cameras, drones, or other technology that captures public behavior constantly in real time would be barred. Legislation on this topic should include the following:
  - » A complete ban on state and local law enforcement from engaging in real-time surveillance of anything other than the interior or immediate surroundings of government buildings.
  - » A ban on contracting with a third-party provider to access real-time surveillance footage of public places.
- The legislature should bar law enforcement from contracting with third-party providers who use facial recognition or AI software to aggregate data on behalf of law enforcement. This will prevent a resurrection of the high-dollar Banjo deal that thankfully fell through in 2020. Legislation should include:
  - » A prohibition on state and local law enforcement contracting with a third-party provider to engage in the early detection of or response to alleged crimes.
  - » A prohibition on purchasing, licensing, or utilizing third-party software that purports to provide law enforcement with enhanced crime detection capabilities using artificial intelligence.

Endnotes

1. Matthew Brooks, "Utah Company Banjo Could Solve Crimes in Seconds," KSLNewsRadio, April 3, 2019, https://kslnewsradio.com/1903497/banjo-artificial-intelligence-police/.
2. Ibid.
3. Ibid.
4. Art Raymond, "Utah A.G. Halts $21 Million Banjo Contract as Founder's Past Ties with KKK Unveiled," *Deseret News*, April 28, 2020, https://www.deseret.com/utah/2020/4/28/21171279/banjo-event-detection-aclu-libertas-surveillance-personal-privacy-kkk-ties-damien-patton-big-brother.
5. Matthew Brooks, "Utah Company Banjo Could Solve Crimes in Seconds," KSLNewsRadio, April 3, 2019, https://kslnewsradio.com/1903497/banjo-artificial-intelligence-police/.
6. Emily Feng, "'Surveillance State' Explores China's Tech and Social Media Control Systems," KPBS Public Media, September 7, 2022, https://www.kpbs.org/news/news/national/2022/09/07/surveillance-state-explores-chinas-tech-and-social-media-control-systems.
7. Ibid.
8. Ibid.
9. Ibid.
10. John Chin and Liza Lin, *Surveillance State: Inside China's Quest to Launch a New Era of Social Control* (New York: St. Martin's Press, 2022).
11. Ibid., 103.
12. Tony Raval, "Council Post: Examining the San Francisco Facial-Recognition Ban," *Forbes*, June 21, 2019, https://www.forbes.com/sites/forbestechcouncil/2019/06/21/examining-the-san-francisco-facial-recognition-ban/.
13. Breed, London. 2022. "Public Safety Priorities for a Safer San Francisco." Medium. July 9, 2022. https://londonbreed.medium.com/public-safety-priorities-for-a-safer-san-francisco-12bf244740d3.

For the remainder of the endnotes, please visit Libertas.org/PB-surveillance

PUBLIC POLICY BRIEF

Securing States and Individuals from Surveillance

LIBERTAS INSTITUTE

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

UTAH CONSTITUTION
ARTICLE I, SEC 27

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