Elizabeth Goitein's Responses to Questions for the Record from Representative Troy Nehls
Hearing of the House Judiciary Committee
"Oversight of the Foreign Intelligence Surveillance Act"
December 11, 2025

1. *What privacy protections exist in instances where surveillance technology, such as facial recognition cameras, are used in public spaces?*

As a constitutional matter, the law on this question is in flux. But it is lagging far behind technological advances, and statutory protections are badly needed to fill the gap.

The Fourth Amendment is triggered when the government invades a "reasonable expectation of privacy." For many decades, courts assumed that people have no reasonable expectation of privacy in actions that they take in public. That assumption, however, is untenable in modern times. The information that the government can glean using advanced technologies — whether a GPS location tracker, a cell site simulator (a.k.a. "Stingray"), or a network of linked surveillance cameras paired with facial recognition technology — far exceeds what an ordinary person can learn from watching another person on the street. These tools can be used to determine a person's identity, habits, associates, and beliefs — information that would otherwise remain functionally private.

The Supreme Court has begun the long process of updating Fourth Amendment doctrine to reflect this reality. In *United States v. Jones* (2012), the Court held that a warrant is required to attach a GPS device to a vehicle and track its movements (largely on public roads) over a four-week period. Although the opinion of the Court focused on the physical trespass involved in affixing the GPS device to a private vehicle, five Justices also concluded that the location tracking itself violated the defendant's reasonable expectations of privacy, with Justice Sotomayor pointing to the "wealth of detail" about "familial, political, professional, religious, and sexual associations" that could be revealed by GPS monitoring. Similarly, in *Carpenter v. United States* (2018), the Court ruled that police needed a warrant to obtain a week's worth of historical cell site location information, notwithstanding the fact that much of the information would reflect the subject's public movements.

Unfortunately, these rulings are limited to the technologies and situations that were before the Court. New technologies are emerging daily and there are countless fact patterns that could arise with respect to their deployment. Facial recognition technology (FRT), a form of artificial intelligence, is a good example of a technology that continues to fall through the legal cracks. FRT can be used to identify and catalog people participating in protests (South Florida police deployed FRT for that purpose), attending houses of worship, entering reproductive care facilities or firearms stores, or engaging in other sensitive activities. In the absence of any federal law governing the use of this invasive technology, states have been attempting to fill the void; many have enacted strong privacy protections that limit the use of FRT by state and local governments. But a significant majority of states still have no legal protections in place, and even the most robust state laws do not address the use of FRT by federal law enforcement or intelligence agencies.

2. *How are law enforcement and national security agencies making use of newly developed surveillance technologies? Which of these technologies are they using?*

A truly dizzying array of surveillance technologies has emerged in the twenty-first century. Cell site simulators can trick cell phones into disclosing their data, including communications data as well as

precise geolocation information. Drones or surveillance cameras that are invisible to pedestrians can be linked with technologies that scan facial features or other biometric indicators — there is even "gait recognition" technology — to identify people in a crowd. As of July 2025, academic researchers were testing a so-called "WhoFi" technology that can track people through walls and in darkness by analyzing how Wi-Fi signals are altered by their presence and movement.

In addition to facial and gait recognition technologies, law enforcement and intelligence agencies are using artificial intelligence (AI) to parse social media for security threats, detect drug smuggling activity at ports of entry, and analyze drone and satellite footage for potential military targets — as well as countless other undisclosed uses. AI is susceptible to discrimination and error, particularly when deployed to perform tasks beyond its technical limitations. The accuracy of facial recognition, for example, degrades significantly when used on dimly lit, obscured, or otherwise poor quality images, and is generally much lower for women and people of color. Natural language processing — a type of AI used to analyze text — is ill-equipped to interpret linguistic nuances such as satire, irony, humor, and slang, and therefore performs poorly on context-sensitive tasks such as identifying "extremist content." Deploying AI for these purposes may end up amplifying racial and ethnic biases, such as by disproportionately linking Muslims to terrorism and violence. These inaccuracies could lead the government to overlook genuine indicators of illicit activity, while misidentifying certain individuals or groups as threats or targets.

If a surveillance technology is available, it is safe to assume that government agencies are using it. However, we have very little information about how the government uses surveillance technologies because there is almost no transparency in this area. Indeed, the government often goes to great lengths to prevent the public from learning about new surveillance technologies and uses. For instance, in the past — and possibly still today — the FBI required state and local law enforcement agencies to sign non-disclosure agreements when purchasing cell site simulators, even forcing them to hide their use of the technology from judges and defense attorneys in court proceedings. Much of what we know about government surveillance practices was revealed by investigative reporting rather than by the government itself.

To fully protect Americans' privacy, Congress should pass technology-neutral laws requiring the government to obtain warrants, court orders, or subpoenas (depending on the nature of the information) in order to collect certain types of information, regardless of the means used. However, technology-neutral legislation is difficult to design, and there is always the chance that the law might fail to capture a new surveillance technology. Moreover, the people of this country have a right to know how the government is collecting and using their personal information. Accordingly, Congress should also require federal agencies to develop and publish policies for the use of any surveillance technologies they adopt, along the lines of New York City's recently-strengthened Public Oversight of Surveillance Technology Act. To further protect Americans' privacy, Congress should also consider requiring government agencies to obtain approval from Congress before adopting new surveillance technologies, as the cities of Boston, MA and Oakland, CA have done.

Congress should require similar transparency for the use of AI by law enforcement and intelligence agencies, and it should codify robust and enforceable rules on how these uses are authorized, tested, and overseen. To start, Congress should build on standards established by the Office of Management and Budget requiring agencies to disclose and mitigate AI's risks to safety and rights, extending them to national security applications of the technology and narrowing the ability of agencies to waive these baseline guardrails.

3. *Do law-abiding American citizens have an option to protect their personal data, such as phone records or location data, private from third party data broker transactions?*

In most states, Americans' privacy is entirely at the mercy of the service providers, apps, and other companies that collect their information in the first instance. Those companies may choose to allow customers to opt out of having their data sold to third-party data brokers—but, of course, many companies do not provide that option (or do little to make users aware of it).

An increasing number of states have consumer data privacy laws that give customers control over whether their data may be sold to third-party data brokers. Some of these laws also restrict the information that companies may collect in the first instance. However, while these laws may have the effect of limiting government agencies' ability to purchase Americans' sensitive information from data brokers, they do not always limit agencies' ability to purchase the information directly from the source companies (e.g., the cell phone service providers or apps). Moreover, even those states that restrict the sale of sensitive data to state and local law enforcement agencies do not restrict access by federal agencies, such as the FBI, DHS, or NSA.

To fully close the data broker loophole that currently allows the government to evade constitutional and statutory privacy protections, Congress must pass legislation. The Fourth Amendment Is Not For Sale Act, which the House passed in 2024, would be a strong start. The legislation would prohibit law enforcement and intelligence agencies from purchasing communications-related and geolocation information (they could still obtain the information with a court order). Additional legislation would be necessary to protect other types of sensitive information, such as health, financial, and biometric data. Such legislation would not prevent law enforcement and intelligence agencies from obtaining the data altogether; it would merely prevent them from buying their way around the standards and processes established in the Constitution and the law.

Ultimately, the best way to stem the flow of Americans' private information to the government is to restrict companies' collection, retention, and disclosure of Americans' information more broadly, through comprehensive consumer data privacy legislation. Unfortunately, the data privacy bills that have been introduced in Congress, such as the American Privacy Rights Act, generally include overbroad exceptions for law enforcement and security purposes. Those exceptions should be narrowed, and/or comprehensive consumer data privacy legislation should be paired with legislation, such as the Fourth Amendment Is Not For Sale Act, limiting government access.