# Quick Guide to the Government Surveillance Reform Act (GSRA)

## Background

On November 7, Sen. Ron Wyden, Sen. Mike Lee, Rep. Warren Davidson, and Rep. Zoe Lofgren introduced the Government Surveillance Reform Act (GSRA), a sweeping bill that would rein in the growing ecosystem of warrantless government surveillance as part of reauthorizing Section 702 of the Foreign Intelligence Surveillance Act (FISA), which is set to expire on December 31.

*For more information, see EPIC's blog post on the GSRA. EPIC has a running blog series on Section 702, where we dive deeper into the authority and the need for significant reform.*

## Key Provisions

- **Fixes the Backdoor Search Loophole [Sec. 101; 302]:** Prohibits warrantless searches for Americans' communications and other protected information, which—in combination with Sec. 601—includes geolocation information, web browsing history, and search history. Applies to information collected under Section 702 (Sec. 101) or under Executive Order 12333 (Sec. 302), and includes several narrow exceptions, such as in some emergency situations and where the search takes place with that American's consent.
    - ***Why it matters:*** *Warrantless backdoor searches have always been one of the most controversial aspects of Section 702. Since the last reauthorization cycle alone, government audits and FISC opinions have revealed staggering abuses of "backdoor searches," including tens of thousands of improper searches relating to civil unrest and significant civil rights abuses.*
- **Strengthens Section 702 Safeguards [Sec. 102-09]:** Limits the use of Section 702 information about Americans to specific national security contexts; repeals the authority to restart "abouts" collection; strengthens several key prohibitions, including on "reverse targeting" and warrantless acquisition of entirely domestic communications; strengthens data retention limits; increases FISA Court oversight of demands for technical assistance from electronic communication service providers; and requires that the purpose of acquisition of information pursuant to Section 702 be to obtain foreign intelligence information, rather than merely a significant purpose.
    - ***Why it matters:*** *Current Section 702 safeguards leave a lot to be desired when it comes to Americans' privacy. These provisions strengthen safeguards already in place for some of the most problematic aspects of Section 702, including by codifying an end to "abouts" collection—which was so plagued with violations that the NSA shuttered it in 2017. By raising the bar on the ban of "reverse targeting," the ban on acquisition of entirely domestic*

*communications, and by requiring that the purpose of acquisition be foreign intelligence information, the GSRA ensures that collection of Americans' communications is kept to a minimum.*

- **Enacts EO 12333 Safeguards [Sec. 301-07]:** Establishes many of the same safeguards for surveillance conducted under EO 12333 as the above sections do for Section 702 surveillance, including a prohibition on backdoor searches, a ban on "reverse targeting" and collection of entirely domestic communications, and robust data retention limits.
    - ***Why it matters:*** *Surveillance conducted under EO 12333 raises many of the same risks as that conducted under Section 702, including the collection, search, and use of Americans' sensitive information. Moreover, EO 12333 surveillance takes place without even the minimal statutory safeguards and judicial review that are present in the FISA context. The GSRA takes a functional approach to protecting Americans' communications and other information by establishing parallel safeguards between Section 702 and EO 12333, rather than a formalistic approach based on where that data is stored.*
- **Closes the Data Broker Loophole [Sec. 304; 508]:** Generally prohibits intelligence and law enforcement agencies from purchasing Americans' data from data brokers under circumstances where they would need some form of a court order to compel that information directly.
    - ***Why it matters:*** *Intelligence and law enforcement agencies have exploited the data broker loophole by warrantlessly purchasing Americans' sensitive information—including location information—from data brokers, circumventing statutory and constitutional protections. These provisions would severely curtail—if not outright prohibit—many of the most harmful government data purchases, such as the widespread purchase of location data, the purchase of non-public personal data from large brokers* and *paid informants, and the use of tools like Clearview AI, which scrape social media profiles in violation of sites' terms of service.*
- **Prohibits Other Forms of Warrantless Foreign Intelligence Surveillance Targeting Americans [Sec. 201]:** Prohibits the government from intentionally targeting—without a warrant—Americans (located inside or outside the United States), as well as any other person reasonably believed to be in the United States for the purpose of acquiring foreign intelligence information under circumstances in which they have a reasonable expectation of privacy or a warrant would be required for law enforcement purposes; establishes a similar requirement for intentional targeting through the use of pen register or trap and trace devices.

- ***Why it matters:*** *These provisions replace Sections 703, 704, and 705 of FISA, which authorize the government to target Americans outside the United States, subject to enhanced protections. The GSRA enhances these protections by extending them regardless of the location of the U.S. person or the location of the acquisition, ensuring that there are consistent—and robust—protections for foreign intelligence surveillance.*

- **Strengthens the FISA Court Processes [Sec. 202-03; 206-09]:** Requires the government to disclose to the FISC all relevant information and certify to the accuracy of its surveillance applications. Consistent with the Lee-Leahy amendment—which passed the Senate in 2020 by a 77-19 vote—the GSRA expands the role of *amici* by expanding their involvement in the FISA Court process, enabling them to appeal FISA Court decisions, and providing them full access to relevant information.
  - ***Why it matters:*** *These certification and accuracy requirements are consistent with prior proposals in response to well-documented failures at the FBI. Given the non-adversarial nature of the FISA Court, these reforms are all the more important. Similarly, while Congress created amici to act as an outside voice, their influence has been hampered by their narrow role.*

- **Ensures Notice and Judicial Review [Sec. 204; 210]:** Clarifies the circumstances in which the government must give notice of surveillance to criminal defendants; establishes grounds for bringing civil claims relating to unlawful surveillance; and establishes that FISA's procedures preempt the state secrets privilege.
  - ***Why it matters:*** *The government has consistently failed to provide notice to criminal defendants, raising questions about "parallel construction." The government has also managed to evade meaningful judicial review by pushing to dismiss cases based on standing or the state secrets privilege.*

- **Strengthens Accountability for Misuse [Sec. 211]:** Requires the FBI, CIA, NSA, and ODNI to establish robust accountability procedures for misuse of surveillance affecting Americans.
  - ***Why it matters:*** *There have been egregious instances of misuse of surveillance authorities, including an NSA analyst searching for the communications of individuals they met on an online dating service or an FBI agent searching for over 19,000 donors to a political campaign. However, it is far from clear what accountability—if any—there has been for agents who abuse their access to these surveillance databases.*

# Quick Guide to the Government Surveillance Reform Act (GSRA)

- **Ends Surveillance Pursuant to Section 215 of the PATRIOT Act [Sec. 205]:** Sunsets a grandfather clause that allows the government to continue certain surveillance pursuant to Section 215 of the PATRIOT Act, which expired in 2020.
    - ***Why it matters:*** *Government reports show that surveillance pursuant to this grandfather clause has grown over the past several years. In 2020, it was revealed that the government used Section 215 to collect web browsing records under a minimal "relevance" standard; per Title V of the GSRA, however, such records would require a warrant.*

- **Reforms the Electronic Communications Privacy Act (ECPA) [Title V]:** Requires law enforcement to obtain a warrant to acquire location information, web browsing records, or search query records; creates consistent protections for call and texting records, whether held by phone companies or app companies; extends the warrant requirement to emails and other stored communications, with some exceptions; harmonizes protections for real-time and historical communications data; and extends consistent protections to data held by the broader universe of parties holding Americans' digital data.
    - ***Why it matters:*** *It has been understood for years that ECPA is in dire need of reform, having failed to keep pace with technological change, new forms of digital data, and the explosion of the data broker industry. These provisions would set more consistent, rigorous standards for acquiring digital information and plug statutory loopholes that law enforcement and data brokers exploit to collect Americans' sensitive information—such as location data—based on outdated distinctions.*

- **Places Safeguards on the Use of Cell-Site Simulators [Title VI]:** Establishes a legal framework for the use of cell-site simulators (also known as Stingrays), including a warrant requirement for their use to conduct surveillance (subject to narrow exceptions).
    - ***Why it matters:*** *Inspector General reports have revealed that government agencies have illegally used cell-site simulators without a court order to obtain real-time cell phone locations. And internal government documents show that the FBI has tried to shield the use of cell-site simulators from discovery in criminal cases by forcing local law enforcement to sign nondisclosure agreements, thereby evading judicial review.*

- **Prohibits Warrantless Surveillance of Car Information [Title VII]:** Requires law enforcement to obtain a warrant for vehicle data, subject to limited exceptions.
    - ***Why it matters:*** *Under Supreme Court precedent, law enforcement can't physically attach a GPS tracking device on a car without a warrant. However,*

*agencies have continued to obtain vehicle location data and other sensitive digital information without a warrant by exploiting loopholes in the law. And it's also clear that companies are eager to sell car location data to intelligence and law enforcement agencies.*

- **Bolsters Oversight of Warrantless Surveillance Programs [Title IV]:** Enhances oversight in a number of important ways, both in the Section 702 context and others; requires a DOJ Inspector General review of certain High Intensity Drug Trafficking Area (HIDTA) surveillance programs.
    - ***Why it matters:*** *Requiring an IG review of HIDTA surveillance programs is particularly important. For example, Hemisphere, a program funded by the Drug Enforcement Agency and the White House's Office of National Drug Control Policy that allows various law enforcement elements—using only subpoenas—to access to billions of phone records of AT&T customers, as well as location information. In combination with Sec. 502, the GSRA would bring programs like Hemisphere under judicial oversight.*
- **Enhances Transparency Requirements [Title VIII]:** In line with other provisions, updates and expands transparency reporting requirements, including certain parallel reporting requirements for EO 12333; permits more granular aggregate reporting by recipients of surveillance orders; requires the PCLOB to report publicly on disparate impacts of surveillance authorities; and requires the government to produce an estimate of incidental collection of Americans' communications pursuant to Section 702.
    - ***Why it matters:*** *Despite some progress in transparency around Section 702 over the years, there remains quite a lot of room for improvement. In particular, the government has reneged on its commitment to provide even an estimate of incidental collection of Americans' communications under Section 702. In the context of EO 12333 surveillance, there's even less public transparency—despite its significant impact on Americans' privacy.*