



U.S. Department of Justice

Criminal Division

Office of Assistant Attorney General

Washington, D.C. 20530

July 14, 2023

The Right Honorable Chloe Smith MP
Secretary of State
Department of Science, Innovation
and Technology (DSIT)
100 Parliament Street
London
United Kingdom
SW1A 2BQ

Dear Secretary of State Smith:

This letter provides a brief overview of the primary investigative tools used to obtain commercial data and other record information from corporations in the United States for criminal law enforcement or public interest (civil and regulatory) purposes, including the access limitations set forth in those authorities.¹ All the legal processes described in this letter are nondiscriminatory in that they are used to obtain information from corporations in the United States, including from companies that will self-certify through the United Kingdom Extension to the EU-U.S. Data Privacy Framework ("UK Extension to the EU-U.S. DPF"), without regard to the nationality or place of residence of the data subject. Further, corporations that receive legal process in the United States may challenge it in court as discussed below.²

Of particular note with respect to the seizure of data by public authorities is the Fourth Amendment to the United States Constitution, which provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported

¹ This overview does not describe the national security investigative tools used by law enforcement in terrorism and other national security investigations, including National Security Letters (NSLs) for certain record information in credit reports, financial records, and electronic subscriber and transaction records, 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, 50 U.S.C. § 3162, and for electronic surveillance, search warrants, business records, and other collection of information pursuant to the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq.

² This letter discusses federal law enforcement and regulatory authorities. Violations of state law are investigated by state law enforcement authorities and are tried in state courts. State law enforcement authorities use warrants and subpoenas issued under state law in essentially the same manner as described herein, but with the possibility that state legal process may be subject to additional protections provided by state constitutions or statutes that exceed those of the U.S. Constitution. State law protections must be at least equal to those of the U.S. Constitution, including but not limited to the Fourth Amendment.

by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. As the United States Supreme Court stated in *Berger v. State of New York*, “[t]he basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.” 388 U.S. 41, 53 (1967) (citing *Camara v. Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967)). In domestic criminal investigations, the Fourth Amendment generally requires law enforcement officers to obtain a court-issued warrant before conducting a search. See *Katz v. United States*, 389 U.S. 347, 357 (1967). Standards for the issuance of a warrant, such as the probable cause and particularity requirements, apply to warrants for physical searches and seizures as well as to warrants for the stored content of electronic communications issued under the Stored Communications Act as discussed below. When the warrant requirement does not apply, government activity is still subject to a “reasonableness” test under the Fourth Amendment. The Constitution itself, therefore, ensures that the U.S. government does not have limitless, or arbitrary, power to seize private information.³

Criminal Law Enforcement Authorities:

Federal prosecutors, who are officials of the Department of Justice (DOJ), and federal investigative agents including agents of the Federal Bureau of Investigation (FBI), a law enforcement agency within DOJ, are able to compel production of documents and other record information from corporations in the United States for criminal investigative purposes through several types of compulsory legal processes, including grand jury subpoenas, administrative subpoenas, and search warrants, and may acquire other communications pursuant to federal criminal wiretap and pen register authorities.

Grand Jury or Trial Subpoenas: Criminal subpoenas are used to support targeted law enforcement investigations. A grand jury subpoena is an official request issued from a grand jury (usually at the request of a federal prosecutor) to support a grand jury investigation into a particular suspected violation of criminal law. Grand juries are an investigative arm of the court and are empaneled by a judge or magistrate. A subpoena may require someone to testify at a proceeding, or to produce or make available business records, electronically stored information, or other tangible items. The information must be relevant to the investigation and the subpoena cannot be unreasonable because it is overbroad, or because it is oppressive or burdensome. A recipient can file a motion to challenge a subpoena based on those grounds. See Fed. R. Crim. P. 17. In limited circumstances, trial subpoenas for documents may be used after the case has been indicted by the grand jury.

Administrative Subpoena Authority: Administrative subpoena authorities may be exercised in criminal or civil investigations. In the criminal law enforcement context, several federal statutes authorize the use of administrative subpoenas to produce or make available business records, electronically stored information, or other tangible items relevant to

³ With respect to the Fourth Amendment principles on safeguarding privacy and security interests that are discussed above, U.S. courts regularly apply those principles to new types of law enforcement investigative tools that are enabled by developments in technology. For example, in 2018 the Supreme Court ruled that the government’s acquisition in a law enforcement investigation of historical cell-site location information from a cell phone company for an extended period of time is a “search” subject to the Fourth Amendment warrant requirement. *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

investigations involving health care fraud, child abuse, Secret Service protection, controlled substance cases, and Inspector General investigations implicating government agencies. If the government seeks to enforce an administrative subpoena in court, the recipient of the administrative subpoena, like the recipient of a grand jury subpoena, can argue that the subpoena is unreasonable because it is overbroad, or because it is oppressive or burdensome.

Court Orders For Pen Register and Trap and Traces: Under criminal pen register and trap-and-trace provisions, law enforcement may obtain a court order to acquire real-time, non-content dialing, routing, addressing, and signaling information about a phone number or email upon certification that the information provided is relevant to a pending criminal investigation. See 18 U.S.C. §§ 3121-3127. The use or installation of such a device outside the law is a federal crime.

Electronic Communications Privacy Act (ECPA): Additional rules govern the government's access to subscriber information, traffic data, and stored content of communications held by internet service providers (also known as "ISPs"), telephone companies, and other third-party service providers, pursuant to Title II of ECPA, also called the Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712. The SCA sets forth a system of statutory privacy rights that limit law enforcement access to data beyond what is required under Constitutional law from customers and subscribers of ISPs. The SCA provides for increasing levels of privacy protections depending on the intrusiveness of the collection. For subscriber registration information, Internet Protocol (IP) addresses and associated time stamps, and billing information, criminal law enforcement authorities must obtain a subpoena. For most other stored, non-content information, such as email headers without the subject line, law enforcement must present specific facts to a judge demonstrating that the requested information is relevant and material to an ongoing criminal investigation. To obtain the stored content of electronic communications, generally, criminal law enforcement authorities must obtain a warrant from a judge based on probable cause to believe the account in question contains evidence of a crime. The SCA also provides for civil liability and criminal penalties.⁴

Court Orders for Surveillance Pursuant to Federal Wiretap Law: Additionally, law enforcement may intercept in real time wire, oral, or electronic communications for criminal investigative purposes pursuant to the federal wiretap law. See 18 U.S.C. §§ 2510-2523. This authority is available only pursuant to a court order in which a judge finds, inter alia, that there is probable cause to believe that the wiretap or electronic interception will produce evidence of a federal crime, or the whereabouts of a fugitive fleeing from prosecution. The statute provides for civil liability and criminal penalties for violations of the wiretapping provisions.

Search Warrant —Fed. R. Crim. P. Rule 41: Law enforcement can physically search premises in the United States when authorized to do so by a judge. Law enforcement must

⁴ In addition, section 2705(b) of the SCA authorizes the government to obtain a court order, based on a demonstrated need for protection from disclosure, prohibiting a communications services provider from voluntarily notifying its users of the receipt of SCA legal process. In October 2017, Deputy Attorney General Rod Rosenstein issued a memorandum to DOJ attorneys and agents setting out guidance to ensure that applications for such protective orders are tailored to the specific facts and concerns of an investigation and establishing a general one-year ceiling on how long an application may seek to delay notice. In May 2022, Deputy Attorney General Lisa Monaco issued supplementary guidance on the topic, which among other matters established internal DOJ approval requirements for applications to extend a protective order beyond the initial one-year period and required the termination of protective orders at the close of an investigation.

demonstrate to the judge based on a showing of probable cause that a crime was committed or is about to be committed and that items connected to the crime are likely to be found in the place specified by the warrant. This authority is often used when a physical search by police of a premise is needed due to the danger that evidence may be destroyed if a subpoena or other production order is served on the corporation. A person subject to a search or whose property is subject to a search may move to suppress evidence obtained or derived from an unlawful search if that evidence is introduced against that person during a criminal trial. See *Mapp v. Ohio*, 367 U.S. 643 (1961). When a data holder is required to disclose data pursuant to a warrant, the compelled party may challenge the requirement to disclose as unduly burdensome. See *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir. 1979) (holding that “due process requires a hearing on the issue of burdensomeness before compelling a telephone company to provide” assistance with a search warrant); *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980) (reaching same conclusion based on court’s supervisory authority).

DOJ Guidelines and Policies: In addition to these Constitutional, statutory, and rule-based limitations on government access to data, the Attorney General has issued guidelines that place further limits on law enforcement access to data, and that also contain privacy and civil liberties protections. For instance, the Attorney General’s Guidelines for Domestic FBI Operations (September 2008) (hereinafter AG FBI Guidelines), available at <http://www.justice.gov/archive/opa/docs/guidelines.pdf>, set limits on use of investigative means to seek information related to investigations that involve federal crimes. These guidelines require that the FBI use the least intrusive investigative methods feasible, taking into account the effect on privacy and civil liberties and the potential damage to reputation. Further, they note that “it is axiomatic that the FBI must conduct its investigations and other activities in a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people.” AG FBI Guidelines at 5. The FBI has implemented these guidelines through the FBI Domestic Investigations and Operations Guide (DIOG), available at <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29>, a comprehensive manual that includes detailed limits on use of investigative tools and guidance to assure that civil liberties and privacy are protected in every investigation. Additional rules and policies that prescribe limitations on the investigative activities of federal prosecutors are set out in the Justice Manual, also available online at <https://www.justice.gov/jm/justice-manual>.

Civil and Regulatory Authorities (Public Interest):

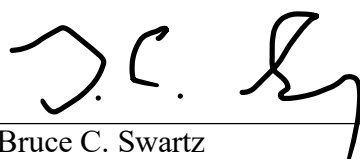
There are also significant limits on civil or regulatory (i.e., “public interest”) access to data held by corporations in the United States. Agencies with civil and regulatory responsibilities may issue subpoenas to corporations for business records, electronically stored information, or other tangible items. These agencies are limited in their exercise of administrative or civil subpoena authority not only by their organic statutes, but also by independent judicial review of subpoenas prior to potential judicial enforcement. See, e.g., Fed. R. Civ. P. 45. Agencies may seek access only to data that is relevant to matters within their scope of authority to regulate. Further, a recipient of an administrative subpoena may challenge the enforcement of that subpoena in court by presenting evidence that the agency has not acted in accordance with basic standards of reasonableness, as discussed earlier.

There are other legal bases for companies to challenge data requests from administrative agencies based on their specific industries and the types of data they possess. For example, financial institutions can challenge administrative subpoenas seeking certain types of information as violations of the Bank Secrecy Act and its implementing regulations. 31 U.S.C. § 5318; 31 C.F.R. Chapter X. Other businesses can rely on the Fair Credit Reporting Act, 15 U.S.C. § 1681b, or a host of other sector specific laws. Misuse of an agency's subpoena authority can result in agency liability, or personal liability for agency officers. See, e.g., Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3423. Courts in the United States thus stand as the guardians against improper regulatory requests and provide independent oversight of federal agency actions.

Finally, any statutory power that administrative authorities have to physically seize records from a company in the United States pursuant to an administrative search must meet requirements based on the Fourth Amendment. See *See v. City of Seattle*, 387 U.S. 541 (1967).

Conclusion:

All law enforcement and regulatory activities in the United States must conform to applicable law, including the U.S. Constitution, statutes, rules, and regulations. Such activities must also comply with applicable policies, including any Attorney General Guidelines governing federal law enforcement activities. The legal framework described above limits the ability of U.S. law enforcement and regulatory agencies to acquire information from corporations in the United States—whether the information concerns U.S. persons or citizens of foreign countries—and in addition permits judicial review of any government requests for data pursuant to these authorities.



Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs