DEPARTMENT OF JUSTICE WHITE PAPER

Sharing Cyberthreat Information Under 18 USC § 2702(a)(3)

Background

Improved information sharing is a critical component of bolstering public and private network owners' and operators' capacity to protect their networks against evolving and increasingly sophisticated cyber threats. As companies continue to adopt the newest technologies, these threats will only become more diverse and difficult to combat. Ensuring that information concerning cyber threats that U.S. companies detect on their domestic networks can be quickly shared will assist those companies in identifying new threats and implementing appropriate preventative cybersecurity measures. But sharing must occur without contravening federal law or the protections afforded individual privacy and civil liberties.

We understand that the private sector would benefit from a better understanding of whether the electronic communications statutes that the Department of Justice (DOJ) routinely interprets and enforces prohibit them from voluntarily sharing useful cybersecurity information with the government. Companies have affirmatively expressed the desire to share information with the government, but have had questions about exactly what information may lawfully be shared. Overly expansive views of what information is prohibited from voluntary disclosure could unnecessarily prevent the sharing of important information that would be used to enhance cybersecurity, thereby thwarting opportunities to address a substantial challenge facing our modern society.

In the interest of advancing discussions in this important area, DOJ has prepared this paper providing its views on whether the Stored Communications Act (18 U.S.C. § 2701 *et seq*.) (SCA) restricts network operators from voluntarily sharing aggregated data with the government that would promote the protection of information systems.[1] We hope that this analysis will help companies make informed decisions about what information legally may be shared with the government to promote cybersecurity.

---

[1] We intend for these views to be of assistance to the public, particularly to those in the legal community who are routinely facing these questions. However, these should not be interpreted to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter by any prospective or actual witnesses or parties. Furthermore, the legal analysis under the relevant statutes is highly fact dependent and any entity engaging in actions that may implicate these statutes should seek its own legal counsel.

Legal Analysis

Issue: Whether the SCA prohibits an electronic communication or remote computing service provider from voluntarily disclosing "aggregate" non-content information to the government.

As a consequence of providing communications services, electronic communications service (ECS)[2] and remote computing service (RCS)[3] providers possess a variety of information that is useful for cybersecurity purposes. Federal law, however, regulates whether and how communications service providers[4] may divulge such information. In particular, the SCA generally prohibits communications service providers "to the public" from disclosing certain types of information. Sections 2702(a)(1) and (2) prohibit the voluntary disclosure of specified content by a provider of ECS or RCS, respectively, to anyone, including a governmental entity,[5] generally unless an exception applies under section 2702(b). In addition, section 2702(a)(3) prohibits communications service providers from disclosing to governmental entities "a record or other information pertaining to a subscriber to or customer of such service," which the SCA specifies does not include the contents of communications. Again, that prohibition generally will apply unless there is an applicable exception under section 2702(c). Thus, communications service providers furnishing services to the public cannot, absent further legal process or another applicable exception, share with the government either specified content or non-content "record[s] or other information pertaining to a subscriber to or customer of such service." A violation of these restrictions does not carry with it criminal liability under the SCA, but it could subject a communications service provider to civil liability under 18 U.S.C. § 2707.

---

[2] An "electronic communication service" is defined to mean "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15); *see id.* § 2711(1) (incorporating, for purposes of the SCA, the definitions in section 2510 of title 18).

[3] A "remote computing service" is defined to mean "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

[4] In many cases, Internet Service Providers (ISPs) will provide both ECS and RCS to their customers. For example, a commercial ISP may serve as an ECS provider with respect to services that permit its users to send and receive electronic mail communications and as an RCS provider with respect to services that allow its users to store and retrieve files or photos on its servers. Because information sharing restrictions apply similarly to ISPs whether they are serving as ECS or RCS providers, this memorandum simply refers to them jointly throughout as "communications service providers."

[5] A "'governmental entity' means a department or agency of the United States or any State or political subdivision thereof." 18 U.S.C. § 2711(4).

The SCA clearly restricts communications service providers from sharing some information they possess as a consequence of providing communications services; however, communications service providers have asked whether non-content aggregate information falls within section 2702(a)(3)'s restriction on sharing "record[s] or other information pertaining to a subscriber to or customer of such [i.e., the ECS or RCS] service." The SCA does not define the scope of information covered by section 2702(a)(3). *See In re Application of the United States of America for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone*, 849 F.Supp.2d 526, 573 (D. Md. 2011) ("The statute offers no definition nor explanation of what constitutes 'records' or 'information pertaining to a subscriber.'"). In particular, it does not expressly address whether information in aggregate form "pertain[s] to a subscriber . . . or customer."

Despite the lack of explicit language in the statute, we believe the SCA's text, structure, purpose, and legislative history, as well as the scope of other federal statutes that regulate the disclosure of customer information by telecommunications companies, support an interpretation of section 2702(a)(3) that would not prohibit a communications service provider from disclosing non-content information to the government that is in aggregate form. That is so, we believe, as long as the aggregation of data results in records or other non-content information that does not identify or otherwise provide information about any particular subscriber or customer. Where information is aggregated but still provides information about a particular subscriber or customer, we believe that section 2702(a)(3) prohibits disclosure to the government.

For example, many of the characteristics of cyber threats can be shared, if they do not pertain to any specific customers or subscribers. Similarly, characteristics of a computer virus or malicious cyber tool that do not divulge subscriber or customer-specific information (*e.g.*, the associated file size, protocol, or port) could be shared. Information about Internet traffic patterns is also susceptible to lawful sharing if divulged in aggregate form. A communications provider could, for example, report to a governmental entity an anomalous swell in certain types of Internet traffic traversing its network or a significant drop in Internet traffic, which could be harbingers of a serious cyber incident.

At the outset, Congress apparently intended for the SCA's restrictions on disclosure of non-content information to be less stringent—or at least less absolute—than restrictions on disclosure of the content of communications. Sections 2702(a)(1) and (2) prohibit a communications service provider from disclosing covered content from a subscriber or customer's communications to *any person*, subject to certain exceptions. In contrast, the restriction in section 2702(a)(3) applies only to disclosure to government entities. Further, and directly relevant to the issue at hand, the restriction in section 2702(a)(3) is explicitly limited to disclosure of only "record[s] or other information *pertaining to a subscriber to or customer of such service*." (Emphasis added). To give appropriate meaning to Congress's inclusion of this specific requirement, the phrase "pertaining to a subscriber . . . or customer" should be interpreted to mean something more exact than any non-content information in an ECS or RCS

provider's possession. *Cf. Organizacion JD Ltda. v. U.S. Dep't of Justice*, 124 F.3d 354, 359-61 (2d Cir. 1997) (interpreting Congress's use of the term "customer" rather than "persons" in the Electronic Communications Privacy Act to intentionally narrow the scope of aggrieved parties who may bring a cause of action under section 2707).

In addition, we note that the SCA refers to "*a* subscriber to or customer of" an ISP rather than "subscribers or customers." This use of the singular noun indicates that Congress was concerned with information that identifies or otherwise provides information about a particular subscriber or customer, rather than information loosely associated with groups of unknown subscribers or customers, such as the total number of a provider's customers, or traffic flow across its network. *Cf. United States v. Hayes*, 555 U.S. 415, 421-22 & n.5 (2009) (treating Congress's use of the singular rather than plural as meaningful when context supports that interpretation).

This interpretation is consistent with the purposes for which the SCA was enacted. The SCA, which was passed as part of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (ECPA), was intended to provide statutory protection for personal privacy rights in light of the "third-party doctrine" endorsed by the Supreme Court in *United States v. Miller*, 425 U.S. 435 (1976). Mindful that, under *Miller*, customer information in the possession of communication service providers might not receive Fourth Amendment protection, Congress enacted the SCA to ensure that such information was not subject to "wrongful use [or] public disclosure by law enforcement authorities [or] unauthorized private parties."[6] S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557. *See also id.* at 3, 5 (stating that "[f]or the person or business whose records are involved, the privacy or proprietary interest in that information should not change" because it is stored or processed by a third-party, and that "Congress must act to protect the privacy of [American] citizens[] . . . [lest it] promote the gradual erosion of this precious right").

Our interpretation of the statute also accords with ECPA's legislative history. As originally enacted, the restriction on disclosing "record[s] or other information pertaining to a subscriber . . . or customer" was found in section 2703, rather than section 2702. *See* ECPA § 201, 100 Stat. at 1862. Describing that provision, the Senate Committee on the Judiciary specifically "noted that the information is information *about the customer's* use of the service not the content of the customer's communications." S. Rep. No. 99-541, at 38. (emphasis added). This statement provides support for the conclusion that Congress intended the phrase "pertaining

---

[6] Under the Fourth Amendment's "third-party doctrine," a party who knowingly reveals information to a third party, "even on the understanding that the communication is confidential," cannot object on Fourth Amendment grounds if the third party provides the information to the government. *S.E.C. v. Jerry T. O'Brien*, 467 U.S. 735, 743 (1984); *Smith v. Maryland*, 442 U.S. 735 (1979).

to a subscriber to or customer of such service" not to cover aggregated data that does not identify or otherwise provide information about a particular subscriber or customer.[7]

Finally, at least two other federal statutes that regulate the disclosure of information possessed by telecommunications providers address the issue of divulging aggregate information. Significantly, both permit the disclosure of aggregate information if it does not identify particular persons or customers, notwithstanding prohibitions they impose on sharing other types of customer information.

Under 47 U.S.C. § 222(a) of the Telecommunications Act of 1996, telecommunications carriers have a duty to protect the confidentiality of proprietary information that belongs and relates to their "customers." Section 222(c)(1) limits the purposes for which a telecommunications provider may use customer proprietary information; however, section 222(c)(3) lifts the general prohibition on the use of such information if it is "aggregate customer information," which is defined to mean "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed." 47 U.S.C. § 222(h)(2).

Similarly, the Cable Communications Privacy Act of 1984 restricts cable service providers' disclosure of "personally identifiable information concerning any subscriber." 47 U.S.C. § 551(c)(1). The statute generally prohibits disclosure of such subscriber information unless an exception applies. Section 551 also carves aggregate information out of its general prohibition, however, by defining "personally identifiable information" to exclude "any record of aggregate data which does not identify particular persons." *Id.* § 551(a)(2)(A).

Section 2702 of Title 18 is analogous to both sections 222 and 551 of Title 47. All three provisions were drafted to regulate the disclosure of information about subscribers or customers held by third-party service providers. In passing each provision, Congress was motivated to safeguard personal information from misuse and unwanted disclosure without imposing restrictions on sharing that would unnecessarily impede competing interests. *Compare* H.R. Rep. No. 104-204, pt. 1, at 90 (1995), *reprinted in* 1995 U.S.S.C.A.N. v. 4, at 56 (balancing "the need for customers to be sure that personal information that carriers may collect is not misused"

---

[7] Sections 2702(a)(3) and 2703(c) both govern how ECS and RCS providers disclose non-content information pertaining to a customer or subscriber: section 2702(a)(3) prohibits an ECS or RCS provider from disclosing non-content information that pertains to its subscribers or customers, whereas section 2703(c) authorizes a governmental entity to compel an ECS or RCS provider to disclose such information pursuant to a warrant, court order, subpoena, or a specified exception. Governmental entities use section 2703(c) during the course of an investigation to obtain records or other information pertaining or related to an ECS or RCS provider's subscribers or customers, including the customers' or subscribers' use of the provider's services, if they are subjects of an investigation, witnesses or victims of a crime, or in possession of evidence or other information associated with the commission of a crime.

against a carrier's need to give its employees relevant information to assist customers with their service), *and* H.R. Rep. No. 98-934, at 30 (1984), *reprinted in* 1984 U.S.S.C.A.N. 4423, 4667 ("It is important that national cable legislation establish a policy to protect the privacy of cable subscribers . . . At the same time, such a policy must also recognize and not unnecessarily impede those flows of information necessary to provide service to the subscribers."), *and* S. Rep. No. 99-541, at 3 ("[The SCA] is modeled . . . to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs.").[8]

Other federal agencies have also interpreted provisions aimed at protecting consumers' privacy to exclude aggregate or "blind" data from general disclosure restrictions, even where the text does not explicitly except such information. For example, the Federal Trade Commission has issued regulations defining "personally identifiable financial information," as used in the Gramm-Leach-Bliley Act, 15 U.S.C. § 6809(4)(A), to exclude "information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses." *See* 16 C.F.R. § 313.3(o)(2)(ii)(B). The FTC adopted this definition even though Congress did not specifically address aggregate data when establishing the parameters for permissible disclosures under the Act. *See* Privacy of Consumer Financial Information, 65 Fed. Reg. 33646 (May 24, 2000) ("An example in § 313.3(o)(2)(ii)(B) clarifies that aggregate information or blind data lacking personal identifiers is not covered by the definition of 'personally identifiable financial information.' The Commission agrees with those commenters who opined that such data, by definition, do not identify any individual."). *See* 16 C.F.R. § 313.3(o)(2)(ii)(B).

* * * * *

Commercial ISPs and other communications service providers may possess large amounts of data, which at the aggregated and abstract level would not pertain to a subscriber or customer. For example, the total number of customers served by an ISP or information representing a provider's network traffic flow and volume by the quantity of bytes and packets observed transiting the provider's networks would not pertain to a subscriber or customer. On the other hand, aggregated information about the total network traffic to or from a particular

---

[8] The explicit carve-outs for aggregate data in other privacy protecting statutes could be read to show that Congress knew how to exclude aggregate data from disclosure prohibitions when it was so minded and, therefore, their absence in section 2702(a)(3) means Congress did not intend aggregate data to be excluded in that provision. However, our interpretation of congressional intent for section 2702(a)(3) leads us to conclude that when Congress enacted ECPA, it was concerned with protecting communications and other information implicating privacy interests. That Congress has elsewhere indicated that it does not regard the disclosure of aggregate data as raising privacy interests that warrant statutory protection weighs in favor of finding that such information is not encompassed by section 2702(a)(3).

static IP address assigned to a customer would be protected under section 2702(a)(3), because that information would reveal facts about that particular customer.

Of course, determining when data does not pertain to a subscriber or customer will be a highly fact-specific inquiry. A provider of ECS or RCS to the public that is making disclosures of non-content/non-customer records to the government should seek legal guidance from its own counsel for specific disclosure determinations to ensure that it is acting consistent with the SCA.

Conclusion

For the reasons described above, we do not believe that the SCA prohibits a provider of ECS or RCS to the public from sharing aggregated non-content data with governmental entities, as long as that aggregated data does not reveal information about a particular customer or subscriber. Reading the SCA to bar communications service providers from disclosing to the government all aggregated data related to providing such services would effectively read out the limitation that the prohibition on disclosure does not cover all records or other information, but only those "pertaining to a subscriber to or customer of such service." We believe such a reading would be inconsistent with the text and structure of the statute, as well as the congressional intent motivating its passage.