Expert Opinion
on the

Current State of U.S. Surveillance Law and Authorities

from

Prof. Stephen I. Vladeck,

University of Texas School of Law

from

15 November 2021

This expert opinion was prepared under the auspices of the Berlin Commissioner for Data Protection and Freedom of Information on behalf of the Conference of Independent Data Protection Supervisors of the Federal Government and the Länder (Data Protection Conference).

The information and views presented in this expert opinion are those of the author. The Conference does not guarantee the accuracy of the data contained in this report. The expert opinion does not bind either the Data Protection Conference or the data protection supervisory authorities of the Federation and the Länder in their assessment of fundamental issues or individual cases.

Further information on the Data Protection Conference:

www.datenschutzkonferenz-online.de

Contact:

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Graurheindorfer Straße 153
53117 Bonn
E-Mail: pressestelle@bfdi.bund.de

SCHOOL OF LAW
THE UNIVERSITY OF TEXAS AT AUSTIN

727 East Dean Keeton Street | Austin, Texas 78705-3299 | (512) 475-9198 | svladeck@law.utexas.edu

STEPHEN I. VLADECK
Charles Alan Wright Chair in Federal Courts

15 November 2021

Matthias Bergt
Leiter Referat I B (Recht)
Berliner Beauftragte für Datenschutz und Informationsfreiheit
Friedrichstraße 219
10969 Berlin, Germany

Re: Memo on Current State of U.S. Surveillance Law and Authorities

Dear Mr. Bergt,

You have asked me to provide my expert opinion in response to a series of questions that have arisen about the current state of U.S. surveillance law and authorities. As you know, I was one of the expert witnesses for Facebook in the *Schrems* litigation before the Irish courts.[1] For reference, I am appending a copy of my expert report in that case to this memorandum (and will refer to it as "Vladeck *Schrems* Report" herein).[2] Among other things, that report also provides a more detailed overview of my qualifications and expertise. *See* Vladeck *Schrems* Report ¶¶ 1–5.

QUESTIONS:

I. ADDITIONAL QUESTIONS REGARDING FISA § 702

1. Does FISA 702 only contain a permission for U.S. intelligence agencies to obtain data from electronic communication service providers, or does it also require electronic communication service providers to disclose data to U.S. intelligence agencies requesting such data or to grant them access to the data?

I address the scope of section 702 of FISA (the centerpiece of the FISA Amendments Act of 2008) in ¶¶ 39–43 of the Vladeck *Schrems* Report. To make a long story short, though, section 702 is compulsory in the sense that, when the United States has issued a directive to an electronic communication service provider that is authorized by its annual certification to the FISA Court under section 702, the provider ***must*** either (1) comply; or (2) challenge the directive in the FISA Court.

1. This analysis in this memorandum represents my best expert opinion on the objective answers to the questions you have asked — and is given entirely without any regard to the interests of *any* particular person, organization, or group.

2. An electronic copy of the report is also available at https://iapp.org/media/pdf/resource_center/Schrems-testimony-Vladeck.pdf.

Put another way, a directive issued under section 702 may require the electronic communication service provider who receives it to disclose data to a U.S. intelligence agency or to grant it access to the data. But it is the ***directive*** that compels the disclosure. Section 702, by itself, does not require electronic communication service providers to proactively disclose data or grant U.S. intelligence agencies general access to data.

2. If the answer to question 1 is that electronic communication service providers are required to disclose or grant access to data: Do U.S. authorities have any means to enforce this obligation? If yes, please describe such means.

Section 702 specifically addresses this question. If the provider challenges the directive in court and loses, its failure to comply with the ensuing court order is expressly punishable by contempt — which could include significant (accumulating) fines. *See* 50 U.S.C. § 1881a(i)(4)(G). If the provider does not challenge the directive in court, but also declines to comply, it can be subject to an adversary judicial proceeding brought in the FISA Court by the Attorney General to enforce the directive. *See id.* § 1881a(i)(5). There, too, if the Attorney General obtains an order compelling compliance, failure to comply is subject to contempt. *See id.* § 1881a(i)(5)(D). Thus, whether the provider (unsuccessfully) challenges the directive or simply refuses to comply, it faces the specter of contempt proceedings (designed to compel its compliance through escalating fines and other remedies) either way.

3. What types of data may the government compel from electronic communication service providers under FISA 702? Does the statute, by its terms, authorize the U.S. government to collect the metadata and content of communications? Does the statute, by its terms, authorize the U.S. government to collect other types or forms of data?

The text of the statute does not speak to the specific types of data subject to acquisition under section 702. But we know that the FISA Court has authorized the collection of both metadata and content of communications pursuant to section 702 under at least some circumstances — meaning that it has formally approved the U.S. government's interpretation of the statute as authorizing such collection. By its terms, the statute does not authorize the U.S. government to collect other types or forms of data — but that does *not* necessarily mean that the government lacks the authority to collect such data. As with content and metadata, it's a question of statutory interpretation for the FISA Court in the first instance. The statute refers only to the "contents" of communications, 50 U.S.C. § 1881a(f)(3)(A), and "contents," as defined in 18 U.S.C. § 2510(8), "when used with respect to any wire, oral, or electronic communication, includes ***any*** information concerning the substance, purport, or meaning of that communication." (emphasis added).

4. Does FISA 702 apply to data in transit and/or to data at rest? Do these two terms together cover all data that may be processed?

Section 702 has been applied to *both* data in transit and data at rest. The in-transit collection is known as "upstream" collection, and the at-rest collection is often described as "downstream" collection. (The PRISM program is an example of the latter.) So far as is publicly known, these two terms ***do*** cover all of the data that may be acquired under section 702, although there **may** be multiple collection programs within these two terms.

5. Which persons or entities are covered by the term "electronic communication service provider" in 50 U.S.C. § 1881(b)(4)?

The definitions in § 1881(b)(4) are exhaustive, but also quite capacious, including:

(A) a telecommunications carrier, as that term is defined in section 153 of title 47;[3]

(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18;[4]

(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18;[5]

---

3. Under 47 U.S.C. § 153(51), "[t]he term 'telecommunications carrier' means any provider of telecommunications services, except that such term does not include aggregators of telecommunications services (as defined in section 226 of this title)." And "telecommunications services" "means the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used." *Id.* § 153(53).

4. Under 18 U.S.C. § 2510(15), "'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications." And "electronic communications" are:

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—
>
> (A) any wire or oral communication;
>
> (B) any communication made through a tone-only paging device;
>
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
>
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

Id. § 2510(12).

5. Under 18 U.S.C. § 2711(2), "the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system."

(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or

(E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

It is difficult to be exhaustive or comprehensive about what each of these definitions encompass, both because they each refer to other statutes with their own definitions and because many of the terms used in these definitions are ambiguous to at least some extent. In this respect, the U.S. legal system functions more like a common law system than a civil law system — in which statutory definitions often invite a fair amount of disagreement and competing (if not conflicting) judicial interpretations. There are some general principles that can be extracted from these definitions (and that I'll attempt to extract below), but the larger point is that many questions of application will yield at least some uncertainties as to the likely result, including (1) whether the U.S. government would ever adopt such an interpretation; and (2) if so, whether a reviewing court would endorse it.

a. In particular: Does the term encompass businesses like banks, airlines, hotels, shipping companies, and the like?

As the above definitions suggest, there are at least some contexts in which banks, airlines, hotels, and shipping companies may well meet at least some of the definitions in § 1881(b)(4). The key possibilities are as providers of electronic communications services (ECS), or remote computing services (RCS). Whether an entity acts as an ECS or an RCS is entirely context-dependent; a determination of whether the ECS regime or RCS regime applies is made based upon the particular service or particular piece of an electronic communication at issue at a specific time and in a specific context. *See, e.g.*, *In re United States*, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009). Thus, to determine whether a company qualifies as an electronic communication service provider, the analysis would separately assess each of the company's different activities under the legal definitions cited above. In practice, only ECS and RCS are likely to be relevant for the businesses you mention. These two definitions should pose few problems in practice — both because their terms are relatively clear and because there is a fair amount of case law resolving some of the ambiguities.

The key point to consider in conducting such analysis is that a company can act as an ECS with respect to *some* communications, an RCS with respect to *other* communications, and neither an ECS nor an RCS with respect to still *other* communications. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1215–16 & n.48 (2004). With that in mind, **yes**, there will be circumstances in which banks, airlines, hotels, and shipping companies *could* all be covered by § 1881(b)(4) — depending upon what services they offer, and to whom. This is all the more true

because the Justice Department has interpreted these terms quite capaciously. *See, e.g.*, Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 117–19 (2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

b. If a business is an "electronic communication service provider" as defined in 50 U.S.C. § 1881(b)(4), is there any law that excludes certain information that the business possesses from collection under FISA 702? For example, is there a law that explicitly states that the status as an "electronic communication service provider" only applies to a certain function a business performs? If, for example, a particular bank is an "electronic communication service provider" under 50 U.S.C. § 1881(b)(4), would FISA 702 allow the U.S. government to collect any communications or data from that bank that was associated with the account of the U.S. government's "target"?

Once a business meets the definition of an "electronic communications service provider" under § 1881(b)(4), there is no law with which I'm familiar that categorically excludes information that the business possesses from collection under section 702. Instead, the question would reduce to whether the communications or data being sought are (1) within the scope of the authorized directive; and (2) not subject to the relevant minimization requirements accompanying the government's certification. Thus, although a business may qualify as an "electronic communications service provider" based upon a very small quantity of activity (and, indeed, activity unrelated to its primary function), the way section 702 is written, that distinction ends up not mattering.

c. 18 U.S.C. § 2711(2) explicitly requires the services mentioned there to be provided to the public. Does this requirement also apply to other kinds of electronic communication service providers under 50 U.S.C. § 1881(b)(4)?

The short answer is "no." Each of the definitions within § 1881(b)(4) are independent — meaning that an "electronic communication service provider" is a company that meets any of the definitions. Per my answer above, the RCS definition (§ 2711(2)) clearly *does* require the provision of services to the public. So, too, the definition of "telecommunication services" in 47 U.S.C. § 153(53). *See ante* at 3 n.3.

But the ECS definition in 18 U.S.C. § 2510(15) is different. That provision defines "electronic communication service" as "*any* service which provides to users thereof the ability to send or receive wire or electronic communications," and includes no requirement that the service be provided to the public or any other third-parties. Thus, for instance, U.S. courts have held that a company meets the ECS definition if it provides e-mail service to its employees. *See, e.g.*, *Fraser* v. *Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114–15 (3d Cir. 2003); *see also Shefts* v.

Petrakis, No. 10-cv-1104, 2011 WL 5930469, at *6 (C.D. Ill. Nov. 29, 2011) ("Authorization to access a 'facility' can be given by the entity providing the electronic communications service, which includes a private employer that provides email service to its employees."). Likewise, a travel agency that provides its agents with computer terminals running an electronic reservation system was also held to be an ECS. *See United States* v. *Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993). Thus, it is possible for a company to meet the definition of "electronic communication service provider" in 50 U.S.C. § 1881(b)(4) *without* providing any services to the public.

d. If one is considering whether a company qualifies as a "remote computing service" under 50 U.S.C. § 1881(b)(4)(C): When are services provided to the public within the meaning of 18 U.S.C. § 2711(2)? E.g., if (1) a company grants its employees or contract workers access to e-mail services (i) for the purposes of conducting the company's business only, and/or (ii) for such employee's or contract worker's private use, and/or (iii) if private use it not permitted but not prosecuted, or (2) a company provides a messaging system to communicate with its clients, e.g. within the online banking system of a bank, does this constitute provision of the services to the public? If one member of a group of companies provides services which would be covered by 50 U.S.C. § 1881(b)(4) to other members of its group of companies but not to any third parties, will such services be regarded to be provided to the public?

The short answer is that none of those examples would likely trigger the definition of a "remote computing service" under § 1881(b)(4)(C). For a good discussion of the purpose of the definition, see *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 310 (E.D.N.Y. 2005) (holding that an airline that operates a website and servers to facilitate communication with its customers is *not* a "remote computing service" under § 2711(2)). *See generally* Kerr, *supra*, at 1229–30 (discussing the RCS definition). An instructive case is *Andersen Consulting, LLP* v. *UOP*, 991 F. Supp. 1041, 1042–43 (N.D. Ill. 1998), which holds that a company is not an RCS solely because it provides access to its internal e-mail system to contractors while working with the company.

More generally, the Senate Report accompanying the Stored Communications Act makes clear that the statute is focused not just on the provision of *services* to "the public," but *"storage or processing* services." 18 U.S.C. § 2711(2). *See generally* S. Rep. No. 99-541, at 8, 10–11 (1986). Thus, it is not enough, as the *JetBlue* case cited above makes clear, that a company provides public-facing messaging platforms, even secure ones. The key is whether the company is providing *to the public* opportunities to store or process data. Thus, a company that provides services to an affiliated company without making those services available on the open market would not meet the *public* part of the definition; and a company

providing nothing more than a mechanism for customers to exchange messages with the company is not providing "storage or processing services."

If the narrowness of this answer seems inconsistent with the breadth of the answer to question 5.c, that is entirely because of the very different definitions of ECS and RCS. RCS, in general, is a much narrower category of services than ECS. That may not matter much to companies that provide both, but it has made a difference in a number of cases where only RCS was at issue, as both the *JetBlue* case cited above, and the cases *it* cites, make clear.

e. All in all: Are there any practical examples of businesses or industries that are not in the scope of 50 U.S.C. § 1881? Which?

As the above answers should make clear, I believe that the answer is yes, but perhaps far fewer businesses and industries than we might think. What may not be obvious from reading section 702 in the abstract is that, at least here, it is borrowing well-worn (and repeatedly interpreted) definitions from the Stored Communications Act of 1986. Congress in that statute was not stealthily trying to treat ***all*** businesses as targetable providers; to the contrary, it was trying to distinguish ***among*** businesses based upon (long-since antiquated) understandings of the different ways businesses used and/or provided communications services. The problem is that those definitions ***themselves*** cover far more businesses today than they did when they were first adopted (and than they arguably were meant to cover). Section 702 exploits those developments.

f. If an entity is not itself subject to FISA 702 but uses an electronic communication service provider to process certain data, is it possible that U.S. intelligence agencies may gain access to such data under FISA 702?

Yes. Insofar as the data is in the possession of the electronic communication service provider, it can be subject to collection under section 702 regardless of whether the data is "owned" or otherwise controlled by an entity other than the provider. That is to say, the question is not where the data comes from; it is whether, at the time the query is run, it is at rest or in motion through the electronic communication service provider's infrastructure.

6. Are U.S. electronic communication service providers and/or Non-U.S. (in particular: EU) subsidiaries of such companies subject to FISA 702 if they process personal data outside the U.S., in particular in the EU/EEA? Does the possession, custody or control principle apply to FISA 702, and if yes, what does this mean? When will a Non-U.S. subsidiary be regarded to be under control of a U.S. entity?

The answer to this question is a bit complicated. On one hand, section 702 is directed at the collection of data from *U.S.* electronic communications service

providers. Indeed, the whole *point* of the statute is to close the gap between the collection of non-U.S. person communications outside the United States (which is governed by Executive Order 12,333) and the collection of U.S. person communications inside the United States (which is governed by "traditional" FISA). If the data at issue is *stored* exclusively by non-U.S. persons outside the United States, it may not fall under section 702 *at all* — and may instead be subject to the less regulated (and far more secretive) surveillance authorities provided by EO 12,333. But if the data is stored by U.S. companies (including EU subsidiaries thereof) outside the United States, it may well fall within the auspices of section 702. After all, that statute only limits collection in cases in which the target is known at the time of acquisition to be in the United States or is a U.S. person. *See* 50 U.S.C. § 1881a(b). Where the target is a non-U.S. person reasonably believed to be outside the United States, and the electronic communication service provider is a U.S. company, there certainly appears to be an argument that section 702 would apply to data stored on European servers — and that the compliance regime outlined above could be used to compel cooperation even with respect to data stored overseas.[6]

7. Can a U.S. electronic communication service provider and/or a Non-U.S. subsidiary of such provider entity prevent the application of FISA 702 by arguing that such application would violate EU or EU member state law?

Not as such, no. Section 702 itself does not condition any of the authorities it provides on whether the collection is consistent with EU or EU member state law; to the contrary, it specifically says that the collection it authorizes is "[n]otwithstanding any other provision of law." 50 U.S.C. § 1881a(a). The only caveat here is Presidential Policy Directive 28 ("PPD-28"), which provides a modicum of protection for certain non-U.S. person data. *See* Vladeck *Schrems* Report ¶¶ 62–64. But PPD-28's limits do not turn on whether the collection is or is not consistent with EU or EU member state law (they turn, instead, on the underlying purposes of the collection). And in any event, PPD-28 does not create any enforceable rights that a U.S. electronic communication service provide or a non-U.S. subsidiary of such a provider could enforce in court.

8. Does FISA 702 apply to Non-U.S. (i.e., not headquartered in the U.S.) electronic communication service providers, e.g. (i) if they do business in the U.S. at all and/or (ii) if they have a subsidiary in the U.S., be it a dependent subsidiary or a legal entity established under U.S. law?

---

6. This issue recently arose in the context of the Stored Communications Act, when Microsoft argued that it could not be required to comply with an SCA order issued by a federal district court in New York for data located on a server in Ireland. *See United States* v. *Microsoft Corp.*, 138 S. Ct. 1186 (2018) (per curiam). Before the Supreme Court could resolve that issue, Congress passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, div. V, §§ 101–106, 132 Stat. 348, 1213 (codified in scattered sections of 18 U.S.C.). *See id*. The CLOUD Act only addresses such acquisition under the SCA, *not* FISA.

At first blush, the way that section 702 is written and has generally been understood, the question is not where the *provider* is located; it's where the *data* is located. Again, that's because, where data of non-U.S. persons is held by non-U.S. companies outside the territorial United States, section 702 does not apply *at all* — and any foreign intelligence surveillance collection is governed instead by Executive Order 12,333 (which, as we've discussed, has advantages and disadvantages).

That said, the U.S. government has, in other contexts (*e.g.*, the Microsoft dispute that led to the CLOUD Act), taken the position that the only relevant consideration is whether the data is in the possession or control of a U.S. communication service provider as defined in 50 U.S.C. § 1881(b)(4). So an EU company with a U.S. subsidiary could well be subject to the section 702 regime, again because of the definition in § 1881(b)(4) includes "agents" of qualifying electronic communications service providers.

Thus, there's no clear, categorical answer to this question. Insofar as the data is at rest on U.S. servers or transiting through U.S. infrastructure, it can be subject to collection under section 702 regardless of where the *company* is that owns the servers and/or the infrastructure. Indeed, if a EU company has a U.S. subsidiary (or itself has a legal presence in the United States), the coercive sanctions discussed above could easily be used to compel compliance with directives under section 702. And insofar as the data is at rest on non-U.S. servers or transiting through non-U.S. infrastructure over which no U.S. company has *any* control, section 702 seems less squarely on point depending upon whether any U.S. company *could* exercise control.

If yes:

a. Does FISA 702 only apply to such subsidiary or company doing business in the U.S., or does the application also extend to the Non-U.S. mother company and/or other affiliates (e.g. a European company processing personal data in the EU that has a subsidiary in the U.S.)?

The definition in § 1881(b)(4) defines "electronic communication service provider" to include "an officer, employee, or agent of an entity" that otherwise meets the statutory definition. 50 U.S.C. § 1881(b)(4)(E). To that end, it is widely understood that a *subsidiary* of an electronic communication service provider counts. But it is not at all clear that a *parent* or *affiliated* company would meet the definition because it is not an agent of its subsidiary / affiliate.

b. If the answer to question 2 is yes: Can obligations to disclose data to U.S. intelligence agencies or to grant access be enforced against Non-U.S. persons or entities? How and to what extent? Would any owner, director, representative, employee or the like run any risk not complying with U.S. requests for disclosure, retention, or access, e.g. the risk of being denied entry to the U.S., of being arrested, of being sanctioned etc.? Could U.S. authorities approach the U.S. subsidiary if the Non-U.S. person or entity does not respond to requests for disclosure or access?

Again, the answer is a bit complicated. Presumably, if the U.S. government is collecting data from servers or infrastructure physically located in the United States, the owner of that material has a legal presence in the United States. Thus, it should follow that the U.S. government could proceed against *whichever* entity has a U.S. presence in order to compel compliance with a directive issued under section 702 along the lines outlined in my response to Question 2, *supra*. To be sure, I have a hard time conceiving of a fact pattern in which the U.S. government could be attempting to acquire data under section 702 from an electronic communication service provider that has *no* footprint in the United States. But it is possible that there could be cases at the margins in which there are non-U.S. companies whose data is at least theoretically subject to acquisition under section 702, but against whom FISA's coercive compliance mechanisms would be ineffective — if for no other reason than the lack of any meaningful legal presence in the United States.

II. FURTHER ACCESS RIGHTS, DISCLOSURE, AND RETENTION OBLIGATIONS

1. Beyond FISA 702, does U.S. law or rules permit authorities (be they intelligence agencies, courts or any other authorities) or other parties in the U.S. to access personal data transferred from Europe to the U.S. while in custody of the intended recipient or by any further recipient to whom the personal data have been disclosed (be they controllers or processors) by either accessing the processing facilities (with or without knowledge of the recipient) or by requiring the recipient to disclose data to the authorities (e.g. FISA 501, national security letters) or to any third party (e.g. pre-trial discovery)?

The short answer to this question is "yes." Local, state, and federal authorities in the United States possess a wide array of legal powers that could, in the right circumstances, legally allow them to collect personal data by either accessing U.S.-based processing facilities or by requiring the recipient to disclose the data to authorities while they are on U.S. soil. These run the gamut from an ordinary search warrant in a criminal case (which are subject to at least 57 distinct sets of laws) to a wiretap (authority for which can come from state or federal law) to a national security letter to a "traditional" FISA warrant. As such, it's going to be difficult to be comprehensive in attempting to answer the following questions about *all* of these authorities. Indeed, it would likely take months to run down each of these authorities one-by-one.

To briefly describe the authorities you've specifically asked about, FISA § 501 is known colloquially as the "business records" (or "tangible things") provision and is codified at 50 U.S.C. § 1861. For a time (from the enactment of the USA PATRIOT Act of 2001 through early last year), this provision provided incredibly broad authority for the federal government to (secretly) obtain non-content information (including telephone metadata) from companies. But the most onerous version of that authority expired in 2020, and has not yet been reauthorized. The version currently on the books is the pre-2001 version, which is far narrower.

National security letters (NSLs) are another example. These are administrative subpoenas issued by the U.S. government to gather information for national security purposes. Unlike FISA § 501, NSLs do not require prior approval from a judge. The Stored Communications Act, Fair Credit Reporting Act, and Right to Financial Privacy Act authorize the U.S. government to seek such information when it is "relevant" to authorized national security investigations. By law, NSLs can request only non-content information, for example, transactional records and phone numbers dialed, but never the content of telephone calls or e-mails.

Pre-trial discovery is both more specific and more open-ended. It's more specific in the sense that it arises only in the context of specific civil litigation — litigation that has *survived* a motion to dismiss. And the discovery must be germane to the factual or legal issues at issue in the specific case. But so long as those things are true, discovery can be quite broad in scope — and *can* include the contents of communications (when not protected by a privilege).

2. Do any U.S. laws, such as 18 U.S.C. § 2703(f), or legal rules, allow the U.S. government or third parties to require a company to retain personal data?

In general, the answer is yes. There are dozens of statutes and federal regulations that require companies to retain specific types of personal, customer, or internal data. But most of these are for purposes at least outwardly unrelated to surveillance and/or intelligence collection. (For instance, maintaining employee records; complying with securities regulation; etc.) There are not nearly as many such laws or rules devoted to the retention of communications that might be acquired under section 702. For one example of the latter, the Federal Communications Commission requires telephone companies to retain certain call records for up to 18 months. *See* 47 C.F.R. § 42.6.

Section 2703(f), which is part of the Stored Communications Act, is perhaps the most relevant and on-point example. Under that statute, "[a] provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process," and shall retain those records for 90 days (a period that can be renewed upon request). 18 U.S.C. § 2703(f). The purpose of the provision is to give the government time to obtain the records through legal process — and the retention requirement can be triggered even through informal requests. *See, e.g.*, *United States* v. *Bach*, No. CRIM.01-221, 2001 WL 1690055, at *1 (D. Minn. Dec. 14, 2001), *rev'd*, 310 F.3d 1063 (8th Cir. 2002). There is no requirement in the statute that the request be for *all* of a company's records. Rather, it seems consistent with the statute that the government could request a company to temporarily retain only a particular subset of records — including, perhaps, records related to a specifically identified employee or customer.

3. If so, please describe in detail such laws or rules referred to in 1. and 2., in particular:

a. Which objectives are pursued by the permission of access or the retention obligation?

I am necessarily generalizing a bit here (again, a comprehensive survey of all of the laws and rules that would satisfy the answers to the first two questions would be quite an undertaking). But most of these laws and rules have one of three objectives: Either the production of evidence in a criminal investigation; the production of information relevant to a counterintelligence investigation; or oversight of particular industries to ensure compliance with civil requirements.

Using § 2703(f) as a particularly apt example, the purpose of the retention requirement is to *allow* the government the ability to pursue requests for the production of such information in a deliberate, timely manner — rather than through expedited, emergency procedures to prevent its destruction.

b. To whom does the law or rule apply?

It varies significantly depending upon which law is at issue. *Most* of the retention requirements apply only to businesses in specific industries (e.g., telephone companies subject to the FCC regulation, or credit reporting agencies covered by the Fair Credit Reporting Act). The Stored Communications Act likewise applies only to certain types of service providers, as in § 2703(f). But search warrants, national security letters, and other comparable authorities can theoretically apply to anyone, or any entity, subject to the jurisdiction of U.S. courts.

c. To what kind of data does the law or rule apply?

The data retention requirements tend to be narrow and specific, e.g., phone companies are required only to retain "the name, address, and telephone number of the caller, telephone number called, date, time and length of the call." The more coercive disclosure rules can apply to far broader classes of data, depending upon the circumstance. Indeed, an ordinary search warrant (which can issue upon a showing of probable cause to believe that a crime has been committed) can, in an appropriate case, be used to obtain virtually *any* data in the recipient's possession.

d. Under what circumstances does the law or rule permit access to (or, as the case may be, retention of) the data?

The retention requirements are typically categorical; when they apply, retention is required. But retention and government access to retained records are entirely ***separate*** legal regimes. Access to data through the more coercive collection processes is more circumscribed. Orders under the SCA and national security letters require at least some kind of showing of an ongoing investigation for which the requested data is relevant. And ordinary search warrants require a judicial determination of probable cause to believe that the search will uncover evidence of a crime. Indeed, part of ***why*** retention requirements are usually given little scrutiny is because the retention requirement, by itself, does not authorize government access; it merely preserves existing sources of records in case the government is able to gain access through conventional means.

e. Which obligations and limitations of the powers granted to the authorities or third parties apply?

In addition to the intrinsic limits on the authorities described above, the coercive acquisition authorities are constrained by a host of external authorities, including the Privacy Act (which governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies) and the Fourth Amendment to the U.S. Constitution (which prohibits "unreasonable" searches and seizures).

f. Are the applicable laws or rules publicly accessible?

So far as I know, yes.

g. Are the applicable laws or rules clear and precise?

For the most part, yes. The Stored Communications Act, as is well known, is a bit outdated with regard to the terminology it uses and the distinctions it draws. *See* Kerr, *supra*. But there is significant case law interpreting the Act that could be brought to bear if and when questions were to arise about its scope.

h. Do U.S. authorities or third parties have any means to enforce such access rights, disclosure obligations, or retention obligations? If yes, please describe such means.

In almost every case, yes. Failure to comply with statutory or regulatory retention obligations subjects the non-complying party to civil sanctions. And failure to comply with a court order compelling disclosure of particular information subjects the non-complying power to contempt — which, again, can include significant (and accumulating) fines.

i. Does the respective law or rule also apply to U.S. persons or entities and/or Non-U.S. (in particular: EU) subsidiaries of such persons or entities if they process personal data outside the U.S., in particular in the EU/EEA? If so, what are the exact requirements?

The answers here vary somewhat among the authorities, but the short version is that at least some of these legal rules do *not* apply to data outside the United States, both in general and because of the strong presumption U.S. courts apply *against* the extraterritorial application of statutes. *See, e.g.*, *RJR Nabisco, Inc.* v. *European Cmty.*, 136 S. Ct. 2090, 2099–100 (2016).

That said, there are significant exceptions. Foremost among them is the 2018 CLOUD Act — which, as noted above, was enacted to specifically address circumstances in which the SCA authorizes the U.S. government to collect data from a company that does business in the United States where the data is stored outside the United States. Although the statute generally authorizes the application of an SCA order to such data, it also provides mechanisms for the companies or the courts to reject or challenge those requests if the request violates the privacy rights

of the foreign country in which the data is stored. (The CLOUD Act also provides for alternative collection through Mutual Legal Assistance Treaties.)

Whether the presumption against extraterritorial application applies to some of the more specific retention authorities identified above, such as 18 U.S.C. § 2703(f), appears to be an open question. Here, much would turn on whether a request to, for example, an EU company to preserve data stored on a U.S. server would even qualify as extraterritorial. If not, then presumably the retention request could run to the EU company without difficulty.

j. Can a U.S. person or entity and/or a Non-U.S. subsidiary of such person or entity prevent the application of such law or rule by arguing that such application would violate EU or EU member state law?

In general, no. But under the CLOUD Act,

> A provider of electronic communication service to the public or remote computing service, including a foreign electronic communication service or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes—
>
> (i) that the customer or subscriber is not a United States person and does not reside in the United States; and
>
> (ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.

18 U.S.C. § 2703(h)(2)(A). A "qualifying foreign government," in turn, is one with which the United States has an agreement specifically under the CLOUD Act and that provides protections similar to those in the CLOUD Act. So far, I believe that only the United Kingdom is a "qualifying foreign government" under this language.

k. Does the respective law or rule apply to Non-U.S. (i.e., not headquartered in the U.S.) persons or entities, e.g. (i) if they do business in the U.S. at all and/or (ii) if they have a subsidiary in the U.S., be it a dependent subsidiary or a legal entity established under U.S. law?

My own research suggests that, in many of the most important cases, the law is unclear on this front. Certainly, retention requests directed to U.S. subsidiaries would turn in no meaningful respect on the fact that the parent company is outside of the United States. But where the request must run directly to the foreign parent, there may be arguments about application of the presumption against extraterritorial application (arguments that simply don't apply to FISA—which is expressly extraterritorial). For instance, a retention request under 18 U.S.C. § 2703(f) might not be one that can be issued to a non-U.S. person — whether formally (because the statute does not apply) or practically (because the recipient faces no realistic sanction for non-compliance). In general, U.S. courts do not have

the power to issue coercive relief against entities outside of their "personal" jurisdiction. So U.S. subsidiaries would be subject to such relief, but parent companies with no presence in the United States would arguably not be.

If yes:

i. Does the law or rule only apply to such subsidiary or company doing business in the U.S., or does the application also extend to the Non-U.S. mother company or other affiliates (e.g. a European company processing personal data in the EU that has a subsidiary in the U.S.)?

Again, there is not a lot of published law to help answer this question. But my reading of the relevant authorities is that the obligation most likely will run only to the subsidiary or company doing business in the United States. 18 U.S.C. § 2703(f) is once again an illustrative example. That provision authorizes retention demands against "electronic communication service providers," a term that, as discussed above, likely would *not* include EU parent companies just because they have US subsidiaries that meet the definition (because of how the term is defined). In that context, the retention request would, both formally and practically, most likely be directed to the company with a true legal presence in the United States — not just because the statutory authority may be *limited* to that authority, but because the government's ability to compel compliance may likewise be limited. But this is not a hard-and-fast rule. The U.S. government could *attempt* to make a retention demand of the EU parent — on the ground that the existence of any legal footprint in the United States would provide the basis for coercive judicial relief. There is a lot of gray here — and it's not obvious to me how courts would rule in such a case, especially if the authority were challenged on extraterritoriality grounds.

ii. Can obligations to disclose or retain data or to grant access be enforced against Non-U.S. persons or entities? How and to what extent? Would any owner, director, representative, employee or the like run any risk not complying with U.S. requests for disclosure, retention, or access, e.g. the risk of being denied entry to the U.S., of being arrested, of being sanctioned etc.? Could U.S. authorities approach the U.S. subsidiary if the Non-U.S. company does not respond to requests for disclosure, retention, or access?

Enforcement is a bit more straightforward. U.S. courts in general lack the ability to issue coercive relief against parties or entities outside their territorial jurisdiction — under the doctrine of "personal jurisdiction." It is certainly conceivable that a U.S. court could use its authority over a U.S. subsidiary to *attempt* to coerce relief against the parent, but it's not clear why the subsidiary wouldn't be able to provide the requested relief itself. Again, the key is that the U.S. entity with a footprint on U.S. soil would be the one subject to potential (and potentially significant) sanctions. And in cases in which there is no U.S. subsidiary, it's not clear how the

U.S. government could obtain any coercive process in U.S. courts against a company with no contacts with the United States.

4. Do any other legal obligations exist that would prevent compliance with the obligations (in particular on confidentiality) in the Standard Contractual Clauses? If so, please describe in detail.

At least based on the old SCCs (and not 2021 SCCs, with which I am less familiar), it's hard to conclusively say that the answer is no given the wide potential array of legal authorities that could come into play. But nothing comes immediately to mind. The central points of dispute involve local, state, and federal government authorities to coercively obtain such information, and those are all addressed (at least in general terms) above.

III. FURTHER PRACTICE

1. Is there a practice of access to or requirement to retain personal data in the U.S. that goes beyond the legal situation to be described in I. and II. above?

I'm not aware of *legal* authorities requiring the retention of personal data that goes beyond my answers above. That said, it is an increasingly common practice among many major U.S. companies, especially those with large customer bases, to *voluntarily* retain significant amounts of customer and transactional data. For the most part, federal law does not *prohibit* such voluntary retention, although it imposes some conditions on how such data is to be stored and used.

IV. REDRESS

1. Is legal redress against access to or retention of their personal data available to all EU/EEA data subjects? If so, please describe the conditions, the limitations and the process. Who will decide on the remedy? If it is not an independent impartial judge elected in a standard process, please describe the deciding body's status, possible dependencies, and the nomination process. Does the deciding body have access to all relevant documents including closed materials? Is the deciding body vested with effective corrective powers? If so, please describe the corrective powers.

As you know, this is the focus of my expert report in the *Schrems* litigation. *See* Vladeck *Schrems* Report ¶¶ 79–103. The short answer is "no" — legal redress against access to or retention of EU/EEA data subjects' data is *not* always available. As my *Schrems* Report explains in some detail, there are a number of oversight and accountability measures designed to ensure that U.S. authorities comply with the statutory and constitutional limits on these powers, and formidable corrective powers for cases in which they do not, *see id.*, but it is not always the case that those measures can be invoked by the data subjects *themselves*.

The one specific counterexample is the Judicial Redress Act of 2016, which is specifically designed to extend privacy protections to EU/EEA nationals. *See id.* ¶¶

66–67. But the Judicial Redress Act doesn't override the intrinsic limits of litigation under the Privacy Act, which, among other things, allows agencies to exempt their records from the Act's disclosure requirements in their entirety in certain circumstances — including when the records are classified in the interest of national security. *See, e.g.*, 5 U.S.C. § 552a(k)(1). The NSA, for instance, has taken advantage of this authority. *See* 32 C.F.R. § 322.7(a) (2016) ("All systems of records maintained by the NSA/CSS and its components shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to 5 U.S.C. 552a(k)(1) to the extent that the system contains any information properly classified under Executive Order 12958 and that is required by Executive Order to be kept secret in the interest of national defense or foreign policy."). Lest it seem like this maneuver is controversial, though, "It is hard to see how it could be otherwise. . . . [I]f the NSA obtains data belonging to a terrorist who is in Paris and may be planning an attack, it should not have to provide the target with access to his files and the ability to correct them," the core purpose of the Privacy Act. Tim Edgar, *Redress for NSA Surveillance: The Devil is in the Details*, LAWFARE, Oct. 19, 2015, https://www.lawfareblog.com/redress-nsa-surveillance-devil-details.

As for the question of "who" decides on the remedy, insofar as these disputes end up in federal court, all of the judges are "Article III" federal judges — meaning that they were appointed by the President and confirmed by the Senate, and hold their offices indefinitely during "good behavior."

2. Does the U.S. government take the position that EU/EEA data subjects outside of the U.S. lack Fourth Amendment rights? What is the scope of the rights that EU/EEA data subjects may be able to vindicate in a judicial proceeding?

The U.S. government usually takes the position that *all* "non-U.S. persons" lack Fourth Amendment rights. *See also, e.g.*, *Agency for Int'l Dev.* v. *Alliance for Open Soc'y Int'l, Inc.*, 140 S. Ct. 2082, 2086 (2020) ("[I]t is long settled as a matter of American constitutional law that foreign citizens outside U. S. territory do not possess rights under the U. S. Constitution."). But as I noted in my *Schrems* Report, there are numerous statutory and non-statutory remedies that are theoretically available to EU/EEA data subjects in at least some of these contexts — including claims that the relevant U.S. authorities have exceeded their *statutory* authority. *See, e.g.*, Vladeck *Schrems* Report ¶¶ 81–83. After all, the successful legal challenge to the bulk collection of telephone metadata brought by the ACLU did not depend upon a constitutional claim, but rather on a claim that the government had exceeded its *statutory* authority — a claim that would be just as available to an EU citizen. *See, e.g.*, *ACLU* v. *Clapper*, 785 F.3d 787 (2d Cir. 2015).

3. May the doctrine of standing function as an obstacle to judicial redress for unlawful surveillance? How?

Yes, but not for the obvious reason. It is axiomatic that those whose data are wrongfully obtained by the government suffer the kind of "injury in fact" that typically satisfies the standing requirement in U.S. federal courts. The problem that

arises in this context is the absence of *notice*. So long as the relevant individual can plausibly allege that his data was wrongfully acquired, he will meet that requirement. *See, e.g.*, *Wikimedia Found.* v. *Nat'l Security Agency*, 857 F.3d 193 (4th Cir. 2017) (upholding a media organization's standing to challenge the legality of "upstream" collection under section 702).

The problem that arises is when, as is usually the case with information obtained through foreign intelligence surveillance authorities, the data that was acquired is classified. *See* Vladeck *Schrems* Report ¶¶ 89–95. In those contexts, because the plaintiff will *not* be able plausibly to allege that his communications were intercepted, he may fail to satisfy standing analysis insofar as he cannot show that the injury he alleges *actually* occurred. *See Clapper* v. *Amnesty Int'l*, 568 U.S. 398 (2013). In that respect, although standing is *an* obstacle, the more significant issue is the difficulty in overcoming the lack of notice — which is more about the state secrets privilege, addressed next, than it is about standing.

4. May the state secrets doctrine function as an obstacle to judicial redress for unlawful surveillance? How?

It is certainly possible, as I explained in my *Schrems* Report. *See* Vladeck *Schrems* Report ¶¶ 100–02. In particular, even if a plaintiff can plausibly allege that his data was unlawfully acquired under one of the U.S. government's foreign intelligence surveillance authorities, his ability to *prove* such acquisition may be foreclosed by his inability to compel the government to turn over classified details about its surveillance activities. An example of this problem can be seen in *Wikimedia Found.* v. *Nat'l Security Agency*, 14 F.4th 276 (4th Cir. 2021). In that case, the Court of Appeals had initially held that Wikimedia had Article III standing to challenge the legality of "upstream" collection under section 702 because it had plausibly alleged that its communications were intercepted. But when it came time for Wikimedia to actually *prove* that its communications had been intercepted, the government invoked the state secrets privilege — and the Fourth Circuit held that the invocation of the privilege made it impossible for Wikimedia to make its case.

On 8 November 2021, the U.S. Supreme Court heard oral argument in *FBI* v. *Fazaga*, the most important case about FISA and the state secrets privilege that the Court has heard in some time. One of the specific questions *Fazaga* raises is whether FISA *overrides* the state secrets privilege in cases in which plaintiffs claim that their communications were unlawfully intercepted in violation of the statute — because it provides a specific process by which courts can consider whether classified information can and should be admitted as evidence (this is why the argument is limited to claims that surveillance is unauthorized by FISA, as opposed to claims that the surveillance is unconstitutional or is unauthorized by Executive Order 12,333). The Ninth Circuit had held that suits arising under FISA are not *subject* to the state secrets privilege because FISA overrides the privilege. Whether and to what extent the state secrets privilege will be an obstacle to judicial redress for unlawful surveillance very much depends upon how the Supreme Court rules in that case. A decision is not likely before May 2022.

* * *

I hope that these answers are useful to you and your colleagues, and would be delighted to discuss any of them further.

Sincerely yours,

Stephen I. Vladeck