CHAPTER 9:

THE BROAD SCOPE OF "ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS" SUBJECT TO SECTION 702

I. Text of the Statute 9-1

II. The Broad Scope of "Electronic Communications Service" under the Electronic Communications Privacy Act 9-1

III. Conclusion 9-3

[1] This Chapter describes US law relevant to determining the scope of what organizations would be affected if US surveillance laws were found to lack adequacy. In privacy discussions in the EU, I have heard the view that Section 702 would apply to a narrow set of companies such as Facebook, but not for transfers between the majority of companies. For example, I have heard that companies engaged in normal commerce, such as an international hotel chain, would not be subject to Section 702 directives.

[2] Upon careful research, this narrow proposed interpretation is not consistent with US law. It is true that requests from the US government under Section 702 apply to data collection from "electronic communications service providers." US law defines "electronic communications service provider" broadly, however. US courts have interpreted the relevant definitions to include any company that provides its employees with corporate email or similar ability to send and receive electronic communications. A finding of inadequate protection that applies to Section 702 would thus apply to almost any company with operations in both the EU and US.

I. Text of the Statute

[3] FISA defines the scope of "electronic communications service providers" subject to Section 702 directives at 50 U.S.C. § 1881. Verbatim, the relevant language of the statute reads:

> (b) Additional Definitions
> (4) Electronic Communication Service Provider – The term "electronic communication service provider" means –
> (A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);
> (B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code;
> (C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code;
> (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).[1]

II. The Broad Scope of "Electronic Communications Service" under the Electronic Communications Privacy Act

[4] The statute applies if a company falls under any of the subsections (A) through (E).[2] The key subsection is (B) for providers of "electronic communication service" under the Electronic Communications Privacy Act.[3]

[1] 50. U.S.C. § 1881(b)(4).
[2] Note the use of the word "or" under subsection (D).
[3] 18 U.S.C. § 2510.

[5] Subsection (A) and (C) are relatively narrow in scope. With regard to subsection (A), a "telecommunications carrier" is any provider of telecommunications services for a fee as defined by the Communications Act of 1934.[4] This provision covers companies such as AT&T, T-Mobile, and Verizon, as they provide telephone services. Regarding subsection (C), a provider of "remote computing service" refers to "the provision to the public of computer storage or processing," as defined by the Stored Communications Act.[5] This definition would again include AT&T, T-Mobile, and Verizon, because they make computer storage available to the general public (for a fee). It would also include Facebook and Google, as they make computer storage available to the general public (often for free).

[6] Subsection (B) is the legal basis for the expansiveness of the definition of the term "electronic communication service provider" in FISA. Subsection (B) makes any company in-scope if it is considered a provider of "electronic communication service" under the Electronic Communications Protection Act (ECPA). **According to the statutory language in the ECPA, a provider of "electronic communication service" is *any* company that provides users "the ability to send or receive wire or electronic communications."**[6]

[7] The courts have applied this statutory language to employer-provided email. The term "electronic communication service" in the ECPA has been applied to any company that provides electronic communications to its employees, irrespective of the primary function of the business.[7] As one example, Nationwide Insurance Company was found to have provided an electronic communication service because it provided its employees with email services.[8]

[8] The courts' interpretation is confirmed by guidance from the US Department of Justice (DOJ). In its 2009 published guide to obtaining electronic evidence, the DOJ states that any company that provides others with the means to communicate electronically, regardless of their primary business or function, can be a provider of electronic communication service under the ECPA.[9] The guidance says "a mere user of [electronic communication services] provided by another is not a provider of ECS." The guide, however, focuses on whether the entity at issue

---

[4] 47 U.S.C. § 153(44); *see also Virgin Islands Telephone Corp. v. FCC*, 198 F.3d 921 (D.C. Cir. 1999), http://law.justia.com/cases/federal/appellate-courts/F3/198/921/597075/.

[5] 18 U.S.C. § 2711(2). In contrast to the broad scope of "electronic communications service" under the ECPA, the leading interpretation of "remote computing service" is narrower and does not include an internal email system of a company, because it is not made available to the public. *See Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041 (N.D. Ill. 1998), https://casetext.com/case/andersen-consulting-llp-v-uop. Other courts have taken a broader view of "remote computing service." *See, e.g., Pure Power Boot Camp v. Warrior Fitness Boot*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008), https://casetext.com/case/pure-power-boot-camp-v-warrior-fitness-boot-camp (ruling that a claim existed against a "remote computing service" regarding emails accessed at work).

[6] 18 U.S.C. § 2510(15). I note that the discussion in this Chapter regards cases that have interpreted the ECPA, not FISA. I am not aware of any reason to believe the use of the term in Section 702 is different. I also am not aware of any declassified FISC opinion that addresses this precise point.

[7] This provision has even been found to apply, for instance, to local governments. In *Bohach v. City of Reno*, the court held that the city fell within the provisions of the ECPA because it provided pager service to its police officers. 932 F. Supp. 1232 (D. Nev. 1996), https://casetext.com/case/bohach-v-city-of-reno.

[8] *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3d Cir. 2004), http://openjurist.org/352/f3d/107/fraser-ra-v-nationwide-mutual-insurance-co.

[9] *See* DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 117-18 (2009), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

provides others with the "means to communicate electronically."[10] It cites the Nationwide case as an example of providing the means to communicate, and cites other included examples such as a business that has a website that offers customers the ability to send messages to third parties.[11]

III. Conclusion

[9] Section 702 and 50 U.S.C § 1881 apply to any "electronic communications service provider." That definition incorporates the definition of any "electronic communications service" under the ECPA, which US courts have interpreted to include any company that provides its employees with corporate email or similar ability to send and receive electronic communications. A finding of inadequate protection based on Section 702 would thus apply to almost any company with operations in both the EU and US.

[10] The EU legal regime as it applies to consent in the employee context means that the broad application of Section 702 may have a particularly strong effect on human resources activities such as internal corporate communications, managing employees, or payroll. Data protection authorities in the EU have been skeptical that individual employees can provide voluntary consent to transfers of their personal data outside of the EU.[12] Furthermore, to the extent consent is valid, it generally remains freely revocable.[13] Companies operating in the EU therefore may face significant challenges in obtaining effective consent from an EU employee to transfer of their personal data to other countries, including the US. Thus, resorting to individual consent as a means of legitimizing transfers in the employment context may not provide effective relief in the face of a finding of inadequacy of protection in the US for Standard Contractual Clauses as a lawful basis for transfer.

---

[10] *Id.* at 117.

[11] *See Becker v. Toca*, 2008 WL 4443050 (E.D. La. Sept. 26, 2008).

[12] The Article 29 Working Party has indicated that when HR data transfers occur as "a necessary and unavoidable consequence of the employment relationship," it would be "misleading" for employers to use consent as a basis because "[i]f it is not possible for the worker to refuse, it is not consent." Thus, "consent will not normally be a way to legitimise [data] processing in the employment context." Article 29 Data Protection Working Party, *Opinion 8/2001 on the Processing of Personal Data in the Emp't Context*, 5062/01/EN/Final WP 48 (Sept. 13, 2001) at 3, 23, 28, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf.

[13] *See id.* at 4 ("[For international transfers,] employers would be ill-advised to rely solely on consent other than in cases where, if consent is subsequently withdrawn, this will not cause problems.").