CHAPTER 1

Big Data: The Conflict Between Protecting Privacy and Securing Nations

Els De Busser

Els De Busser

Senior Lecturer, European Criminal Law; Senior Researcher, Centre of Expertise Cyber Security, The Hague University of Applied Sciences

Law enforcement and intelligence agencies need to comply with specific legal frameworks when gathering and processing personal data for the purposes of criminal investigations and national security. Private companies need to comply with specific legal frameworks when gathering and processing personal data for the purpose of commercial activities.

Both law enforcement and intelligence agencies, as well as multinational private companies, engage in cross-border data gathering. This means that two countries' legal frameworks could be applicable to their activities: one in the territory where the data are gathered and another in the territory where the data are processed—for example, personal data gathered in the European Union (EU) but processed or stored in the United States. Another conflict can arise even amongst laws in the same country—i.e., laws applicable to personal data gathered for the purpose of commercial activities versus laws applicable to personal data processed for the purpose of criminal investigations/intelligence activities.

When two or more legal frameworks contain conflicting provisions or requirements, it can create confusing situations for law enforcement or intelligence agencies and private companies. Two developments have added to the confusion. The first is the continuously increasing digitalization of the way citizens communicate, purchase items, manage finances, and do other common activities, which increase the possibility that law enforcement and intelligence authorities may need this information in the context of an investigation. The second is the growing use by private companies of cloud storage and servers located in other jurisdictions.

The last decade has shown that this dilemma is more than just theoretical. Both territorial and material conflicts have surfaced in the last several years. Fundamentally different data protection legal frameworks, combined with intensive cooperation in criminal and intelligence matters in the EU and United States, have contributed to this dilemma. In the aftermath of

the September 11, 2001, attacks on US territory, two types of data transfers were set up between the EU and the United States. First, in 2002, the US Bureau of Customs and Border Protection requested passenger name record data (PNR data) from EU air carriers flying to airports located in the United States. Then, in 2006, journalists revealed that Belgium-based private company SWIFT had transferred financial messaging data—including personal data—to the US Department of the Treasury for the purpose of investigations into the financing of terrorist activities. In both cases, agreements were ultimately signed to offer a legal framework for such transfers. In 2016, a ruling by the US Court of Appeals for the Second Circuit Court drew much attention from the industry when it ruled in favor of Microsoft in a case against the US government challenging a warrant for personal data held on a server located in Ireland.[4]

This paper focuses on these territorial conflicts, the mechanisms for preventing or solving related conflicts of laws, and the implications for relevant stakeholders.

National Laws

Criminal and national security investigations are traditionally regulated on a national level. Data protection and privacy are also typically covered in national and regional laws. Criminal law—especially criminal procedure—is traditionally regulated at the national level due to its inherent connection to the political and historical identity of a country. Hence, EU institutions have only limited competence to regulate criminal law. National security is regulated exclusively on a national level as it relates to the protection of the country and its citizens from national crises.

Data protection and privacy laws tend to be regulated on a national level as well, often in line with a regionally binding legal framework, such as the Council of Europe's (CoE) Convention 108[5] and the EU's legal instruments. Nevertheless, we can see different ways of regulating privacy and data protection. In 1999, Banisar and Davies distinguished four models: comprehensive laws, sector-specific laws, self-regulation, and technologies of privacy.[6] Whereas in Europe the first model of comprehensive or umbrella laws is clearly the preferred one, the United States uses a combination of the three other models. Apart from binding laws and rules, we should not overlook the importance of non-binding guidelines on privacy and data protection. Both the United Nations (UN) and the Organisation for Economic Co-operation and Development (OECD) have developed such rules. Of these two, the OECD's "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" is the only set of guidelines that includes a paragraph on conflict of laws.[7]

With regard to the binding legal frameworks on data protection, the aforementioned CoE Convention 108 is the widest in territorial scope as well as the most generally formulated set of standards on data protection that—in spite of the Convention currently going through a modernization—remain valid.[8]

The two most relevant[9] EU legal instruments based on the CoE standards are Directive 95/46/EC[10] covering data processing in commercial activities, and Framework Decision 2008/677/JHA[11] covering

4 On January 24, 2017, the Second Circuit Court of Appeals denied the US Department of Justice's petition for a rehearing.

5 Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the Convention)," January 28, 1981, ETS No. 108, http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.

6 Daniel Banisar and Simon Davies, "Global trends in privacy protection: an international survey of privacy, data protection and surveillance laws and developments," *J. Marshall J. Computer & Info. L.*, 18 (1999): 13-14 and William J. Long and M.P. Quek, "Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise," *Journal of European Public Policy,* 9 (2002): 330.

7 OECD, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 2013, http://www.oecd.org/sti/ieconomy/privacy.htm.

8 The draft protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was finalized by the responsible Ad Hoc Committee on Data Protection on June 15-16, 2016, and is awaiting adoption by the CoE Committee of Ministers following consultation of the Parliamentary Assembly. For the full text of the draft protocol, see: CoE, September 2016, "Draft Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data," https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a616c.

9 These legal instruments are considered most relevant because they cover the two widest categories of data processing: processing for commercial purposes and processing for law enforcement purposes. Further legal instruments covering data protection are Regulation (EC) No 45/2001, "On The Protection Of Individuals With Regard To The Processing Of Personal Data By The Community Institutions And Bodies And On The Free Movement Of Such Data," *Official Journal of the European Communities*, L 8, January 12, 2001; Directive 2002/58/EC, "Concerning The Processing Of Personal Data And The Protection Of Privacy In The Electronic Communications Sector," *Official Journal of the European Communities,* L 201 , July 31, 2002, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:en:PDF.

10 Directive 95/46/EC, "On the Protection of Individuals with Regard to the Processing of Personal Data and On the Free Movement of Such Data," *Official Journal of the European Communities*, L 281, November 23, 1995, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF.

11 Framework Decision 2008/977/JHA, "On the Protection of Personal Data Processed in the Framework of Police and

data processing for the purpose of criminal investigations and prosecutions. Both are being replaced by two newly adopted legal instruments: 1) the General Data Protection Regulation (GDPR)[12] covering data processing in commercial activities, which will be effective as of May 25, 2018; and 2) the directive on the protection of natural persons "with regard to the processing of personal data by competent authorities for the purposes" of "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" and on "the free movement of such data" (directive on data protection for law enforcement purposes),[13] which will be effective as of May 6, 2018.

A significant aspect of the new GDPR is its expanded territorial application. The GDPR applies to companies that have no establishment in the EU but direct their activities at or monitor the behavior of EU citizens. This expanded scope will lengthen the list of companies from countries outside the EU—such as US companies active on the EU market—that will be confronted soon with a set of EU legal provisions with which they need to comply. One legal provision included in the GDPR that gained attention from US companies is the "right to be forgotten," which really is a right to have personal data removed when it is no longer accurate, adequate, or relevant, or if it is excessive. Thus, it is not an absolute "right to be forgotten" as the catchphrase may make one believe. The right to have inaccurate, inadequate, irrelevant, or excessive data removed has always been a right under European data protection standards, but a 2014 Court of Justice[14] ruling requiring Google to remove links containing personal data inspired a more specific "right to erasure" provision in the GDPR.[15]

The reform of the EU legal instruments on data protection also implied an expansion of the territorial scope of the directive on data protection for law enforcement purposes. The first instrument on law enforcement data protection, the 2008 Framework Decision—since expanded—covered only personal data exchanged between the member states; domestically collected data were excluded. The latter was governed only by national law. The scope of the new directive does include domestically gathered data, which means that both data transfers within the EU and data transfers outside the EU are regulated by the same directive.

"The right to have inaccurate, inadequate, irrelevant, or excessive data removed has always been a right under European data protection standards. . ."

Unlike the EU, the United States has approximately twenty sector-specific or medium-specific[16] national privacy or data security laws as well as hundreds of such laws among its states and its territories.[17] Examples of national sector-specific privacy and data protection laws include the 1996 Health Insurance Portability and Accountability Act,[18] regulating the processing and disclosure of protected health information, and the 1999 Financial Services Modernization Act,[19] also known as the Gramm-Leach-Bliley Act (GLBA), requiring financial institutions to provide their customers with a privacy notice.

With respect to criminal investigations, the US Fourth Amendment offers privacy safeguards, such as a warrant requirement, when law enforcement and intelligence authorities gather data. However, the warrant requirement, which necessitates a showing of probable cause, can slow things down. Quicker ways of obtaining data outside the scope of Fourth Amendment searches are administrative subpoenas and national security letters (NSLs). For an administrative subpoena, a warrant is not

Judicial Cooperation in Criminal Matters," *Official Journal of the European Union,* L350, December 30, 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF.

12 Regulation (EU) 2016/679, GDPR, *Official Journal of the European Union*, L 119, May 4, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC.

13 Directive (EU) 2016/680, *Official Journal of the European Union,* L 119, May 4, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC.

14 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, Case C-131/12, May 13, 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

15 GDPR, Article 17.

16 Privacy or data security laws focused on a specific medium—for example an electronic medium—rather than a certain industry sector.

17 DLA Piper, "Data Protection Laws of the World, 2016, 503.

18 Health Insurance Portability And Accountability Act of 1996, Public Law (Pub.L.) 104–191, August 21, 1996, https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

19 Gramm–Leach–Bliley Act, Pub.L. 106–102, November 12, 1999, https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.

Members of the European Parliament vote on the EU Passenger Name Record (PNR) Directive, which would oblige airlines to hand EU countries their passengers' data in order to help the authorities to fight terrorism and serious crimes. *Photo credit:* Reuters/Vincent Kessler.

required; rather, it is sufficient for the subpoena to be reasonable and give opportunity for the individual (hereafter, "data subject") to receive a judicial review of its reasonableness.[20] Administrative subpoenas can be used by federal agencies to order an individual to appear or deliver documents or items. The statute granting this power describes the circumstances under which subpoenas may be issued.[21]

Likewise, the 2001 USA Patriot Act[22] expanded the use of NSLs, so that any government agency investigating or analyzing international terrorism can use them.[23] Government agencies responsible for certain foreign intelligence investigations can issue NSLs to obtain customer transaction data from communication providers, banks, and credit agencies for the purpose of national security investigations.[24] The 2015 USA Freedom Act[25] strengthened judicial review of NSLs and restricted bulk collection of communications or financial records.[26] It is the use of NSLs and subpoenas in an extraterritorial manner that has caused conflicts of laws between the EU and the United States.

20 Laura K. Donahue, "Anglo-American Privacy and Surveillance," *J. Crim. L. & Criminology* 96 (2006): 1109 (footnote 278). Charles Doyle, *Administrative subpoenas in criminal investigations: a sketch*, CRS Report for Congress, March 17, 2006, https://fas.org/sgp/crs/intel/RS22407.pdf.

21 Charles Doyle, *Administrative subpoenas in criminal investigations*.

22 Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (USA Patriot Act) Act Of 2001, Pub.L. 107–56, October 26, 2001, https://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf.

23 Charles Doyle, National Security Letters in Foreign Intelligence Investigations: Legal Background, CRS Report for Congress, July 30, 2015, https://fas.org/sgp/crs/intel/RL33320.pdf.

24 Ibid.

25 USA Freedom Act, Publ.L. 114-23.

26 Charles Doyle, *National Security Letters in Foreign Intelligence Investigations*.

This brings us to the main differences facing two entities often involved in cross-border data flows and in the resulting conflict of laws between the EU and the United States. The first difference is the model of data protection legal framework that is used. The EU's reliance on omnibus legislation stands in stark contrast to the American system of sector- and data-specific laws, self-regulation, and privacy technologies. Secondly, the substance of data protection laws tends to differ between the EU and the United States. That does not mean that one offers higher data protection than the other; it means that protection is differently organized and different elements of protection are prioritized. These differences make the exchange of personal data between jurisdictions a challenge. Transferring personal data from one country to the other for the purpose of a criminal investigation or a national security investigation heightens the challenge, since such transfers should comply with two sets of data protection laws as well as two sets of criminal laws or national security laws.

Conflicts of Laws

As mentioned above, the EU and US data protection legal frameworks have led to several conflicts between the two systems. A request for EU-based personal data from US authorities would put EU companies in a dilemma. Refusing to comply with the request would trigger consequences in the United States, but complying with it may violate EU data protection laws. This section focuses on the instruments used for requesting personal data and some of the conflicts that have arisen.

Direct Access

Direct access to data is the most intrusive type of instrument for one country to obtain data held by another country, as it touches upon the sovereignty of the country granting access. Additionally, the country granting access wishes to retain some kind of control over the processing of its data by the other country. For these reasons, both countries involved will have to reach a prior agreement on the circumstances under which direct access can be allowed.

Direct access to PNR data, before those passengers board a flight from the EU to any US destination, was the subject of a number of PNR agreements between 2004 and 2012. The reason for the request for direct access was a pre-screening process that used to be conducted by US air carriers. In 2001,[27] the Aviation and Transportation Security Act moved the authority to perform a pre-screening process of passengers to the Department of Homeland Security (DHS). When the Aviation and Transportation Security Act was expanded by the 2004 Intelligence Reform and Terrorism Prevention Act,[28] an agreement with the EU became necessary due to the requirement that the European Commission (EC) assess the data protection laws of a non-EU country before a transfer of EU personal data can take place. If the EC determines that the data protection law(s) in the recipient country are not adequate, appropriate safeguards must be agreed upon. With respect to PNR data, this led to arduous negotiations between EU and US representatives resulting in several successive agreements,[29] with the most recent concluded in 2012.[30] The negotiations were complex—the main issues were the types of data included in the pre-screening, the purpose for which they would be used, and the time limits for storing the data. Another key discussion point was direct access. Giving a country *direct* access to the databases of another country's air carriers (in this case a region of twenty-eight member states) amounts to a significant sovereignty issue. When compared with a request for data or even a warrant for data, the problem was the unspecified and large amount of data.

One of the data protection standards applicable in the CoE, and thus in the EU, is the purpose limitation principle and the necessity requirement that is inherently connected to it. This means that the gathering of personal data should be done only for a specific and legitimate purpose. Processing for a purpose that is incompatible with the original purpose is not allowed unless the following conditions are met: the processing should be provided for by law, it should be necessary, and it should be proportionate. The necessity requirement includes those cases in which personal data need to be processed for the purpose of the suppression of criminal offenses. This allows, in particular, the use—by law enforcement authorities—of data that were previously gathered in a commercial setting such as data related to the purchase of an airline ticket. The necessity requirement implies, however, that the data are necessary in a specific criminal investigation, and thus mass collection of data is not considered necessary, even if such data could be useful.

27 Aviation and Transportation Security Act, Public Law no. 107-71, November 19, 2001.

28 See Section 7210, Exchange of Terrorist Information and Increased Preinspection at Foreign Airports, Intelligence Reform and Terrorism Prevention Act of 2004, Public Law no. 108-458, December 17, 2004.

29 For an overview, see Els De Busser, *EU-US Data Protection Cooperation in Criminal Matters* (Antwerp: Maklu, 2009), 358-384.

30 Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security (PNR Agreement), *Official Journal*, L 215, August 11, 20121, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22012A0811(01).

The purpose limitation principle is known in the United States as well. It is, however, not a general principle in the American system, but is included in specific laws only; however, while these laws may be specific, they can nonetheless have a relatively wide scope such as the 1974 Privacy Act.

For compliance with the EU data protection standard of purpose limitation, the method of accessing the data—the "push" or "pull" method—is therefore crucial. The push method means that only the data that are necessary for the purposes of a specific investigation are sent by the EU air carriers to the US Department of Homeland Security. The pull method would allow access by DHS to the air carriers' databases to retrieve the data needed. The pull method is considered the more intrusive method, taking into account that direct access to a database is granted to another country. The difference between the methods can be described as the equivalent of giving the keys to one's home to another person—the pull method—versus giving another person exactly what is necessary from one's home—the push method. The 2012 PNR agreement provides that air carriers shall be required to transfer PNR to DHS using the less intrusive push method.[31]

Subpoenas

US authorities can rely on administrative subpoenas[32] for obtaining data from private companies for the purpose of an investigation into international terrorism.[33] The conditions under which these subpoenas can be issued are laid down in statutes such as the aforementioned 1996 Health Insurance Portability and Accountability Act or the 1999 Gramm-Leach-Bliley Act (GLBA).[34] The latter protects customers' financial data including account numbers and bank balances. Financial institutions based outside the United States, but offering products or services to US customers, must also comply with the GLBA including by giving citizens a privacy notice explaining how their data would be processed.

In the aftermath of the September 11, 2001, attacks, efforts increased to investigate the financing of terrorism by setting up the Terrorist Finance Tracking Program (TFTP) of the US Treasury Department. Belgium-based SWIFT company is not a bank and does not handle money; however, it handles the financial messaging data instructing banks to transfer a specific amount of money in a specific currency from one account to another. As SWIFT organizes the majority of worldwide money transfers, it was the ideal partner for the US Treasury Department when investigating the financing of terrorism under the TFTP. The targeted data held by SWIFT included personal data. When media coverage revealed that personal data from EU citizens had been transferred from SWIFT's EU servers in the Netherlands to the US Treasury Department following what was described as "non-individualized mass requests,"[35] the European Commission and the Belgian Privacy Commission stepped in. SWIFT had been complying with US subpoenas in order to avoid prosecution in a US court, but this policy had breached Belgian data protection law. This resulted in a procedure before the Belgian Privacy Commission and in a new EU-US agreement, which provided a compromise on the safeguards for data transfers for the purposes of the Terrorist Finance Tracking Program, also known as the TFTP Agreement.[36]

Warrants

The Fourth Amendment requires probable cause for warrants issued to collect personal data for the purpose of criminal investigations, although exceptions apply.[37] Obtaining a warrant is slower in comparison to a subpoena, but offers more protection to the person involved. In the context of private companies supplying data to law enforcement, the 1986 Stored Communications Act (SCA)[38] allows the government to obtain a warrant requiring an electronic communication service provider to produce data such as customer information, emails, and other materials provided

31 Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security (PNR Agreement), Article 15.

32 Charles Doyle, *Administrative subpoenas in criminal investigations*.

33 See, The International Emergency Economic Powers Act (IEEPA), which followed the signing by President George W. Bush of Executive Order 13224, "Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism," 50 USC § 1702, September 23, 2001.

34 Gramm–Leach–Bliley Act, Pub.L. 106–102, November 12, 1999.

35 Belgian Data Protection Commission, Opinion no. 37/2006, Opinion on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas, September 27, 2006.

36 Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *Official Journal of the European Union*, L 195, July 27, 2010, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ%3AL%3A2010%3A195%3ATOC.

37 Applicable US legislation is 18 USC Chapter 109 and Rule 41 of the Federal Rules of Criminal Procedure.

38 Required disclosure of customer communications or records, 18 US Code (USC) § 2703, https://www.law.cornell.edu/uscode/text/18/2703.

that probable cause is shown.[39] SCA warrants are not typical warrants but have some characteristics of subpoenas and are referred to as "hybrids." The latter means that the warrant is obtained upon showing probable cause, but it "is executed like a subpoena" since "it is served on the provider and does not involve government agents entering the premises" of the provider "to search its servers and seize the e-mail account in question."[40] The matter raises questions regarding the extraterritoriality of such hybrid warrants.

That was exactly the concern in the recent Microsoft case. In 2014, when Microsoft was served with an SCA warrant for obtaining data on an email account that was located on the company's server in Ireland, the US District Court denied Microsoft's attempt to quash the warrant by stating that "even when applied to information that is stored in servers abroad, an SCA Warrant does not violate the presumption against extraterritorial application of American law."[41] Microsoft appealed and received wide support from the industry in the form of several amicus curiae briefs. On July 14, 2016, the Second Circuit Court of Appeals ruled in favor of Microsoft by limiting the SCA warrants to data held within the United States regardless of whether the data pertain to a US citizen or not. It is relevant to point out here that it is unknown whether the data subject is a US citizen or not. However, the Microsoft case is not over yet; on October 13, 2016, the US government filed a petition for a rehearing,[42] and the reasons given are of essential importance for the extraterritorial seizing of data. In the appeal ruling, the Second Circuit Court acted on the assumption that providers know exactly where data are stored. The government's petition clarifies that this is not always the case[43] and stresses that due to companies working with changing facilities in different locations worldwide, "critical evidence of crimes now rests entirely outside the reach of any law enforcement anywhere in the world, and the randomness of where within an intricate web of servers the requested content resides at a particular moment determines its accessibility to law enforcement."[44]

On January 24, 2017, the appellate court denied the petition in a 4-4 vote, confirming the ruling in favor of Microsoft. Whether the case will be submitted before the Supreme Court is, at this moment, unknown. The only current alternative is a time-consuming mutual legal assistance request—but even this is not always possible due to the limited list of bilateral agreements. Scholars are expecting Congress to pass laws giving extraterritorial applicability to US warrants,[45] much like the Belgian law allowing for the extraterritorial collection of data in a criminal investigation with a *post factum* approval of the target country. Note that the CoE Cybercrime Convention allows for extraterritorial collection of data, provided that consent of the person who has the lawful authority to disclose the data is obtained.[46]

National Security Letters

Issued by high-ranking officials for the purpose of national security investigations,[47] National Security Letters are orders allowing law enforcement and intelligence agencies to obtain data by avoiding the requirements of the Fourth Amendment. Certain US laws allow for the use of NSLs[48] to order private companies such as banks, phone companies, and Internet service providers to hand over "non-content information." What can be produced in response to an NSL are log data including phone numbers or email addresses of senders and receivers, as well as information stored by banks, credit unions, and credit card companies. These disclosures may still

39 Recent cases, "In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (US District Court New York, 2014)," *Harvard Law Review*, 128 (2015): 1019.

40 In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (United States District Court, SDNY, 2014), 25.4.2014, 12, https://casetext.com/case/in-re-of-184.

41 Ibid.

42 US Court of Appeals for the Second Circuit, No. 14-2985, In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation.

43 See also Orin Kerr, "The surprising implications of the Microsoft/Ireland warrant case," *Washington Post*, November 29, 2016, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case/?utm_term=.b12c9264b191.

44 US Court of Appeals for the Second Circuit, No. 14-2985, In the Matter of a Warrant to Search.

45 See Jennifer Daskal, "A proposed fix to the Microsoft Ireland Case," *Just Security*, January 27, 2017, Microsoft v US, 2nd US Circuit Court of Appeals, No. 14-2985; Jennifer Daskal, "Congress needs to fix our outdated email privacy law," *Slate*, January 26, 2017, http://www.slate.com/articles/technology/ future_tense/2017/01/the_confusing_court_case_over_microsoft_data_on_servers_in_ireland.html; and Centre for Democracy and Technology, "Latest Microsoft-Ireland case ruling affirms U.S. warrants do not reach data stored outside the U.S.," January 26, 2017, https://cdt.org/press/latest-microsoft-ireland-case-ruling-affirms-u-s-warrants-do-not-reach-data-stored-outside-the-u-s/.

46 Council of Europe, Cybercrime Convention, ETS No. 185, November 23, 2001, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

47 50 USC §436, Requests by Authorized Investigative Agencies, and 438, Definitions.

48 The Fair Credit Reporting Act, the Electronic Communication Privacy Act and the Right to Financial Privacy Act.

include personal data that identify or enable the identification of an individual.

From an EU perspective, NSLs are problematic because they do not require probable cause; rather, the data must be relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. Due to the purpose limitation principle and the requirement for necessity and proportionality, the use of an NSL in the EU is highly questionable.

". . . [C]onflicts of laws create legal uncertainty and confusion for law enforcement and intelligence agencies."

In addition, the GDPR creates severe difficulties for the use of NSLs by US authorities. US companies will fall within the territorial scope of the GDPR when they offer goods or services to citizens in the EU—regardless of whether payment is required—so even free social media services such as Facebook are included. US companies will also be subject to EU jurisdiction if they monitor the behavior of EU citizens within the EU.[49] This will have a number of consequences.

First, NSLs often come with gag orders prohibiting the recipient of the NSL from disclosing their existence. The GDPR, however, introduces higher transparency standards for personal data. Thus, NSLs with a gag order requesting data on EU citizens become difficult due to these transparency rules. Article 14 of the GDPR thus creates a conflict of laws. The article lists the information that the data controller shall provide to the data subject in case personal data are processed that were not obtained directly from the data subject. The information to be provided includes the "purposes of the processing for which the data are intended [and] the legal basis for the processing; the recipients of the data" and, where applicable, that "the controller intends to transfer personal data to a [recipient in a] third country or international" organization.[50] Such transparency requirements make gag orders sent by US authorities to EU data subjects infeasible.

Second, Article 23 of the GDPR allows for restrictions to its other provisions. The duty to inform the data subject when the data were accessed for the purpose of criminal or national security investigations can also be restricted. However, such restriction is dependent on the member states or the EU creating a separate legislative measure. In order to protect the secrecy that goes with criminal and national security investigations, we can anticipate that member states will be providing for this exception in their national laws. That means that the scope of the exception, and whether or not this will include foreign law enforcement requests, is left to the member states' discretion. The relevance for private companies lies in the fines for non-compliance with Article 14 of the GDPR, which requires companies to notify the data subject. Companies that fail to comply with the GDPR risk an administrative fine of up to €20 million or up to 4 percent of the total worldwide annual turnover, whichever is higher. This means that if a US company offering electronic communications in the EU market receives an NSL with a gag order,[51] to transfer personal data to a Federal Bureau of Investigation (FBI) field office, the effect of the gag order will depend on the national law of the EU member state in which the US company has its EU headquarters. If such member state's national law provides for an exception to Article 14 for criminal investigations and national security purposes, the gag order could be upheld. If not, the company would violate the gag order if it informed the data subject to comply with Article 14, thereby facing a fine of up to €20 million or 4 percent of its total worldwide annual turnover.

Implications of Conflicts of Laws

As illustrated above, conflicts of laws create legal uncertainty and confusion for law enforcement and intelligence agencies, whose efforts in collecting cross-border information and intelligence could be blocked. If they proceed, they risk collecting information that would be inadmissible as evidence in a later criminal trial. For those countries that follow the "fruit of the poisonous tree doctrine,"[52]

49 GDPR, Article 3, §2.

50 Directive (EU) 2016/680, On The Protection Of Natural Persons With Regard To The Processing Of Personal Data By Competent Authorities For The Purposes Of The Prevention, Investigation, Detection Or Prosecution Of Criminal Offences Or The Execution Of Criminal Penalties, And On The Free Movement Of Such Data, And Repealing Council Framework Decision 2008/977/JHA, *Official Journal of the European Union*, L 119, May 4, 2016.

51 In accordance with 18 USC 2709—which was inserted by the Patriot Act—wire or electronic communications providers have a duty to comply with requests for subscriber information and toll billing records information, or electronic communication transactional records in their custody or possession. These requests can be made by the Director of the FBI as defined by 18 USC 2709. The provision concerns stored data, and not data in transit. This is relevant since the standards for obtaining stored data by the FBI are lower—NSLs do not require judicial review—than they are for data in transit—to be obtained by search warrant.

52 The fruit of the poisonous tree doctrine is a theory on the admissibility of evidence upheld by some EU member states. It means that evidence that infringes on the right to a private life is inadmissible *and* that all evidence that derived from it is also

all evidence derived from such inadmissible evidence likewise cannot be used in court. This outcome is a waste of time and resources as well as a discouragement for law enforcement and intelligence agencies.

For companies offering goods or services in several countries, conflicting laws may pose an expensive problem. In addition to regulatory fines, which are direct costs, indirect costs include legal expenses and the effect on reputation when the company is taken to court for non-compliance with—for example—a subpoena in one country because it complied with another country's law. The aforementioned Microsoft case illustrates that such proceedings can take a significant amount of time.

Citizens whose personal data are at the heart of these conflicts might have their data processed in accordance with a law that is contradictory to the law that they know. This can result in unlawful processing from their point of view. In addition, it can be problematic for such individuals to submit a complaint or initiate a proceeding in the country where the unlawful processing took place. For example, the lack of judicial redress for EU citizens under the 1974 US Privacy Act resulted in years of negotiations and ultimately led the US Congress to pass the 2016 Judicial Redress Act.[53]

Answers to Conflicts of Laws

Ad Hoc Agreements and Adequacy Requirement

Ad hoc agreements, which can resolve conflicts by presenting a hierarchy between conflicting laws and provisions, offer a possible solution. Several agreements were concluded in the past decades between EU and US authorities covering the exchange of personal data, but the EU required the United States to have an adequate level of data protection before any exchange could take place.

After the entry into force of Directive 95/46/EC, any transfer of personal data to a third country had to be preceded by an assessment of the recipient country's level of data protection. If the level of data protection was not considered adequate, the transfer would not happen unless appropriate safeguards for processing the data were in place.[54] Because the US level of data protection was not considered adequate and in order to maintain trade, a compromise was reached consisting of the self-certification system called the Safe Harbor agreement.[55] After Safe Harbor's annulment by the Court of Justice of the EU in 2015,[56] the EU-US Privacy Shield replaced it.[57]

Box 1.1. Is the adequacy requirement a form of extraterritorial application of EU legal provisions on data protection?

In essence, the adequacy requirement attaches a condition to a transfer of personal data in order to protect these data from being processed by a third state's companies or authorities in a manner that would be considered unlawful under the EU legal framework. Defining extraterritorial application of legal provisions as the interference with another state's sovereignty, we can state that the adequacy requirement to a certain extent constitutes extraterritorial application. There is an extraterritorial effect since the EU essentially imposes its level of data protection on certain third states. However, the effect is limited; if a third state does not pass the adequacy test, the transfer of data does not happen or appropriate safeguards can be agreed upon. If both parties—the EU member state transferring personal data and the recipient third state that did not pass the adequacy test—agree on such safeguards, there really is no extraterritorial application of EU legal provisions, but rather a bilateral agreement.

Ad hoc agreements can offer a solution for the conflict of laws in the context of a particular transfer of data, but they do not offer general solutions for all data transfers. Examples of ad hoc agreements are the 2012 PNR Agreement[58] and the 2010 TFTP Agreement.[59] Both these agreements, together

inadmissible. For example if during a house search, a laptop containing criminal information is seized without proper legal authority, this criminal evidence will be inadmissible if the house search was conducted illegally.

53 House Resolution (HR)1428—Judicial Redress Act of 2015, https://www.congress.gov/bill/114th-congress/house-bill/1428.

54 EU Directive, Articles 25 and 26 of Directive 95/46/EC, Data Protection Commissioner, https://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapters-3-to-7-Final-Provisions/94.htm.

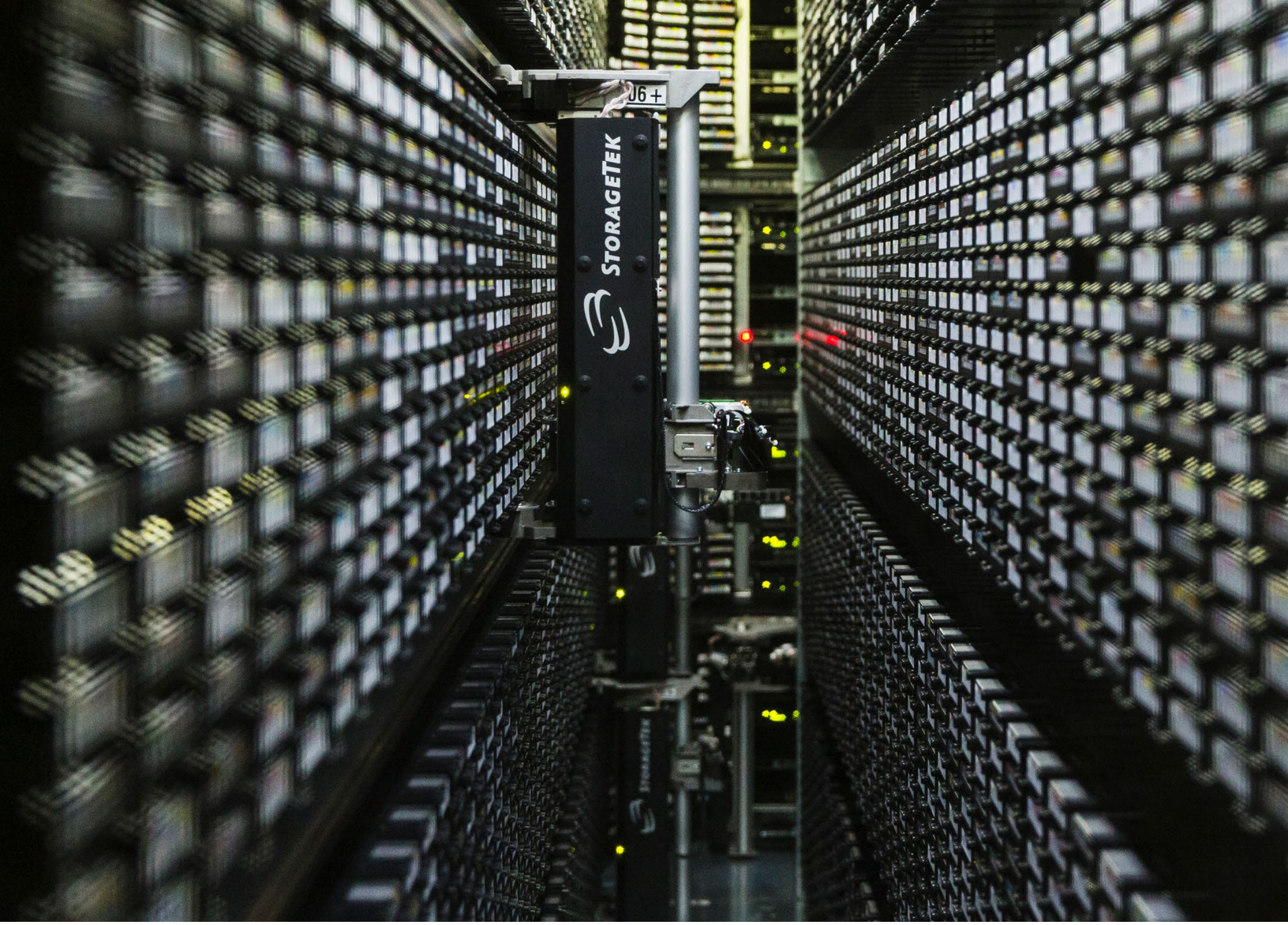
55 European Commission, Commission Decision, *Official Journal*, L 215, August 25, 2000.

56 Judgement of the Court (Grand Chamber), Schrems v Data Protection Commissioner, C-362/14, October 6, 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362.

57 Commission Implementing Decision (EU) 2016/1250, On the Adequacy of the Protection Provided by the EU-US Privacy Shield, *Official Journal*, L 207, August 1, 2016.

58 Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, *Official Journal*, L 215, August 11, 2012.

59 Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *Official Journal*, L 195, July 27, 2010.



A robotic tape library used for mass storage of digital data is pictured at the Konrad-Zuse Centre for applied mathematics and computer science (ZIB), in Berlin. *Photo credit:* Reuters/Thomas Peter.

with the 2003 EU-US mutual legal assistance agreement,[60] the 2002 Europol-US Agreement,[61] and the 2006 Eurojust-US Agreement,[62] were complemented with the 2016 agreement between the United States and the EU on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses.[63] This "Umbrella Agreement" offers a "superstructure" to the prior agreements, consisting of a set of safeguards protecting data exchanged under the terms of the agreements. Most importantly, the European Commission made the signing of the Umbrella Agreement dependent on the adoption of the US Judicial Redress Act.[64] The latter expands the scope of the 1974 Privacy Act to non-US citizens, allowing them to challenge the processing of their personal data by US authorities via court redress.

Supervision by Courts and Supervisory Authorities

The aforementioned Microsoft case shows that judges, at times, rely on laws that were adopted decades ago, when a global communication infrastructure and cloud service providers were not envisioned by the legislator. Today, judges should interpret such laws and are faced with new questions on the extraterritorial obtaining of data. Supervisory authorities will also continue to play a

60 *Official Journal of the European Union,* L 181, July 19, 2003.

61 Supplemental Agreement between the Europol Police Office and the United States of America on the exchange of personal data and related information, December 20, 2002 (not published in the *Official Journal*).

62 Agreement between Eurojust and the United States of America, November 6, 2006 (not published in the *Official Journal*).

63 Agreement on mutual legal assistance between the European Union and the United States of America, *Official Journal of the European Union*, L 336, December 10, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:336:FULL.

64 House Resolution 1428—Judicial Redress Act of 2015, February 1, 2016, https://www.congress.gov/bill/114th-congress/house-bill/1428.

role in how data transfers work in practice under the GDPR. They will continue to advise national parliaments and governments on legislative and administrative measures related to personal data processing, promote awareness of data controllers and processors of their obligations, handle complaints, and ensure consistent application and enforcement of the GDPR.

International Guidelines

The OECD guidelines described earlier are the only non-binding rules that explicitly refer to potential conflicts of data protection and privacy laws. Even though it was of essential importance that the expert group charged with developing the OECD guidelines paid attention to the issue, no detailed solution was offered. Rather, the guidelines recommend that countries work toward their own solutions. Nevertheless, the expert group mentioned a few possible solutions in the explanatory note to the guidelines.[65] Two of the solutions suggested by the expert group are highlighted here.

The expert group, first of all, stated that identifying one or more connecting factors that, at best, indicate one applicable law, is one way of approaching the issue. Connecting factors would have to be multiple and precise. Left imprecise, they would not solve the issues described earlier, for example, in the Microsoft case.[66]

A second indication offered by the expert group is to make a distinct choice for the law offering the best protection of personal data. As much as this could be a morally valuable criterion, the question is: how does one define "best protection"? When considering systems like those of the United States and the EU, where protections take different forms, the criterion of best protection could be defined only by means of general requirements including the presence of supervisory authorities, judicial complaint mechanisms, transparency, etc. Using general requirements for deciding on the most protective system defies the purpose, because both countries will fulfill the requirements—e.g., the presence of supervisory authorities—but with their own version of them.

Mutual Legal Assistance

Why do countries rely on tools involving direct access, extraterritorial subpoenas, and warrants when a request-based cooperation mechanism—based on mutual legal assistance treaties—has been in place for several decades? Mutual legal assistance in criminal matters no longer seems to be part of the narrative. Mutual legal assistance has the reputation of being slow and leaves substantial discretion to the state receiving the request in finding grounds for refusing the request.[67] In addition, mutual legal assistance requests are linked to a specific criminal investigation, leaving no chance for a bulk transfer of data.[68]

Could the solution to these difficulties lie in one expanded mutual legal assistance treaty? The idea is not that far-fetched and was even raised in the aforementioned Microsoft case,[69] but it would require significant investments in speeding up the system of mutual legal assistance requests. Investments would be needed in creating new legal provisions on allowing direct and secure communication between authorities from different countries but also in human resources to handle mutual assistance requests. One suggestion that lies along the same line of reasoning is expanding the CoE Cybercrime Convention[70] to include more types of criminal offenses.[71]

Recommendations

As described above, national rather than regional laws are the primary binding legal instruments for data protection and criminal or national security investigations.

Traditionally, ad hoc agreements have been used in an attempt to bridge conflicts of laws, but they have triggered difficult and protracted negotiations, leaving the parties and affected citizens in legal uncertainty for quite some time. Likewise, the existing mutual legal assistance mechanisms are unpopular since they do not bring quick results in a context where fast responses are essential. There are possible alternatives, however, which include the following:

65 OECD, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 2013, "Explanatory Memorandum," http://www.oecd.org/sti/ieconomy/privacy.htm.

66 Data controlled by Microsoft as a US company but sitting on a server located in Ireland have a clear connection with both the United States (data controller) and Ireland (data location). Thus, more precise connecting factors than data control or location are necessary in order to decide on one country's law.

67 See also Jennifer Daskal, "The Un-Territoriality of Data," *Yale Law Journal*, 125 (2015): 393.

68 The latter has been at the heart of PNR data and the TFTP Agreement discussions, due to the EU's "necessity" and "proportionality" requirements.

69 Brief for Appellant, 16, In re Warrant to Search a certain E-mail Account Controlled & Maintained by Microsoft Corp., No. 14-2985-CV, (2d Circuit, December 8, 2014).

70 Council of Europe, Convention on Cybercrime, Articles 17-18, ETS No. 185, November 23, 2001.

71 Jennifer Daskal, The Un-Territoriality of Data, *Yale Law Journal*, 125 (2015): 394.

- Create a variation to request-based cooperation that functions in a more efficient and effective way. This would mean that responding to requests for personal data from other countries would become more automatic; however, this type of arrangement implies some form of "blind" recognition of other countries' national security and data protection regimes. The EU mutual recognition system demonstrates that such a system may fail when mutual trust among participating countries is deficient.
- Create international guidelines with a list of criteria for determining which law applies when a conflict of laws emerges. International guidelines seem feasible and attainable using the OECD guidelines as a benchmark. These guidelines should allow personal data located abroad to be obtained fast, efficiently, and most importantly, with due protection for the data subject's rights.
    - Such criteria should be established either at a supranational level—i.e., by an authority that either has the competence to legislate in a manner that legally binds the participating countries—or by means of an agreement that is ratified by countries. In the latter option, countries would commit themselves to complying with these criteria in handling extraterritorial data requests for the purpose of criminal investigations and national security investigations. An example could be taken from Article 32 of the Cybercrime Convention, but the guidance would need to be more specific with respect to consent.
    - Given the challenges of supranational fora, such as the EU, for regulating criminal and national security matters, a non-binding set of criteria may be a good option. Drawing on the adequacy decisions under Article 45 of the GDPR, the criteria should include, at a minimum, effective and enforceable data subject rights; effective administrative and judicial redress for data subjects; and one or more independent and effective supervisory authorities.[72]

Conclusion

The exponentially expanding volume of digital data creates new challenges for criminal and national security investigations. There is a tension between the need for digital data for the purpose of such investigations and the need to respect a country's sovereignty in order to protect the privacy of its citizens. Any solution to these challenges will also have to take into account the speed with which data are needed for the purpose of a criminal or national security investigation and the fact that the data might be hard to locate.

72 GDPR, Article 45.