CHAPTER 4:

SYSTEMIC SAFEGUARDS FOR LAW ENFORCEMENT

[1] This Chapter describes safeguards in the US criminal justice system, as contrasted with the safeguards for foreign intelligence investigations discussed in Chapter 3. As discussed elsewhere in the Testimony, a wiretap or other government collection of electronic communications in the US takes place primarily either under law enforcement or foreign intelligence legal authorities.[1] For collection in the US, Executive Order 12,333 does not apply.[2]

[2] This Chapter first provides an overview of US criminal procedure, highlighting the numerous safeguards built into the Constitution's Bill of Rights. Drawing on my current academic research, it then discusses eight ways in which the safeguards in the US are usually more substantial than the safeguards that apply within the EU.

I. Overview of US Criminal Procedure

[3] The criminal justice system in the US was shaped by the experience of the generation that fought the American Revolution in the 1770s and 1780s. This generation rallied against what it considered violations of their fundamental rights by the British King George III. The US Constitution, and especially the Bill of Rights (the first ten amendments), provides numerous safeguards against the government in criminal cases. These safeguards include:

1. The Fourth Amendment prohibits unreasonable searches or seizures, and generally requires probable cause of a crime, and a warrant overseen by an independent magistrate.[3]

2. The Fifth Amendment prohibits compelled testimony against oneself, provides protections of a grand jury, prohibits two trials for the same crime, and assures due process generally.[4]

[1] When these searches occur under a mandatory order, they follow either the foreign intelligence or law enforcement regime. Section 1802(a) of Title 50 of the U.S. Code permits a limited collection for a period of a year or less, at the direction of the President and with the approval of the Attorney General, for (1) the collection of communications exclusively between or among foreign powers; and (2) the collection of technical intelligence, which does not include spoken communications of individuals, from property under the control of a foreign power. The government can also gain access to electronic communications with consent.

[2] To be explicit, my assumption in writing this Testimony is that the Court is considering the adequacy of protection for data that is transferred to the US, and not for data that remains in the EU. Based on that assumption, I focus my analysis on the legal rules that apply to data transfers. By contrast, Executive Order 12,333 applies to data collected outside of the US.

[3] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

[4] *Id.* amend. V ("No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.").

3. The Sixth Amendment assures the right to a speedy and public jury trial, to be informed of the nature of the accusation, to confront adverse witnesses, and to have legal counsel.[5]

4. The Eighth Amendment protects the individual against excessive bail, and against cruel and unusual punishments.[6]

[4] These rights apply to both US persons and non-US persons facing a criminal trial in the US. In the over two centuries since the US Constitution went into effect, the Supreme Court has elaborated on many of these rights, such as the right of an individual to a lawyer supplied by the state if the defendant cannot afford a lawyer.

II. Eight Specific Safeguards in US Law Enforcement Investigations

[5] As part of my ongoing academic research, I am now in the editing stage of two articles. The Emory Law Journal article is entitled "Why Both the EU and the U.S. are Stricter than Each Other for the Privacy of Government Requests for Information."[7] The Wisconsin International Law Review article is entitled: "A Mutual Legal Assistance Case Study: the United States and France."[8]

[6] The Emory Law Journal article describes how the EU is "stricter" (more substantial), especially in having a comprehensive approach to data protection – the current Data Protection Directive, and the upcoming application of the General Data Protection Regulation for commercial data and the new Directive on law enforcement data processing.[9] In my experience, this relative "strictness" of the EU with respect to data protection, as measured by the comprehensiveness of the written law, is widely accepted.

---

[5] *Id.* amend. VI ("In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense.").

[6] *Id.* amend. VIII ("Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishments inflicted.").

[7] I presented the symposium version of this research in March 2016, before I was aware that I would be asked to participate in this case. The main points in the draft article and this Chapter are the same as those in the March symposium presentation. DeBrae Kennedy-Mayo, a Research Associate at Georgia Tech, is co-author for this law review article.

[8] My co-authors and I agreed to write the article, and drafted the article, before I was aware that I would be asked to participate in this case. The co-authors are Justin Hemmings, who until recently was a Research Associate at Georgia Tech, and Suzanne Vergnolle, a French doctoral student in comparative privacy law who was resident at Georgia Tech in 2015-16.

[9] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 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, 2016 O.J. (L 119) 89, http://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2016%3A119%3ATOC&uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG.

[7] My research supports the less-widely understood conclusion that the US is "stricter" (more substantial) than the EU in multiple respects in the area of criminal procedure safeguards. Specifically, the Emory Law Journal article identifies eight ways in which the US often or usually exceeds the EU protections:

A. Oversight of searches by independent judicial officers;

B. Probable cause of a crime as a relatively strict requirement for both physical and digital searches;

C. Even stricter requirements for government use of telephone wiretaps and other real-time interception;

D. The exclusionary rule, preventing prosecutors' use of evidence that was illegally obtained, and civil suits;

E. Other legal standards that are relatively strict for government access in many non-search situations, such as the judge-supervised "reasonable and articulable suspicion" standard under ECPA;

F. Transparency requirements, such as notice to the service provider of the legal basis for a request;

G. Lack of data retention requirements for Internet communications; and

H. Lack of limits on use of strong encryption.

A. Oversight of Searches by Independent Judicial Officers

[8] Standard practice in the US is that search warrants are issued by a judge, who is a member of the judiciary and not part of the executive branch. Federal judges have strong legal guarantees of independence – Article III of the US Constitution guarantees that federal judges have lifetime tenure, and cannot have their salaries reduced.[10]

[9] This review by an independent judge, separate from the executive branch, is far from universal under European legal systems. Approximately half of the Member States lack review by an independent judge when the government seeks to engage in surveillance.[11] As discussed in

[10] U.S. CONST. art. III. More specifically, the constitutional text provides that federal judges retain their positions during "good behaviour," which means in practice that they have lifetime tenure except in extraordinary circumstances, notably when Congress impeaches the individual judge. *Id.*; *see* Walter F. Pratt, *Judicial Disability and the Good Behavior Clause*, 85 YALE L.J. 706 (1976), http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1164&context=law_faculty_scholarship.

[11] European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights, Safeguards, and Remedies in the European Union* at 52 (Nov. 2015), http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf [hereinafter FRA Report]. Even in the United Kingdom, which shares a common law history with the US, the independent judiciary plays a far smaller role in overseeing criminal investigations than in the US. The Regulation of

our Wisconsin International Law Journal article, French public prosecutors typically combine the prosecutorial and judicial roles when determining what evidence to gather for a criminal prosecution.[12]

B. Probable Cause of a Crime as a Relatively Strict Requirement for Both Physical and Digital Searches

[10] Most important for surveillance issues, the Fourth Amendment limits the US government's ability to conduct searches and seizures, and warrants can issue only with independent review by a judge. The Fourth Amendment governs more than simply a person's home or body; its protections apply specifically to communications, covering a person's "papers and effects."[13] In criminal prosecutions, the law enforcement officer must determine whether the Fourth Amendment requires a warrant to conduct a search, or whether it is an instance where a lesser requirement will satisfy the reasonableness requirement of the Fourth Amendment.[14] If law enforcement officers are incorrect in their assessment, the evidence collected may be excluded from evidence in a criminal trial.

[11] The search warrant is issued by a neutral magistrate, a judge, only after a showing of probable cause that there is incriminating evidence in the place to be searched. Probable cause that a crime has been committed must be established by the law enforcement officer by "reasonably trustworthy information" that is sufficient to cause a reasonably prudent person to believe that an offense has been or is being committed or that evidence will be found in the place that is to be searched.[15] In the warrant, the law enforcement officer is required to list, with specificity, the items to be searched and/or seized.[16]

C. Even Stricter Requirements for Government Use of Telephone Wiretaps and Other Real-time Interception

[12] In U.S. law, the real-time interception of electronic data is recognized as holding the greatest privacy risks, and consequently an order authorizing such interception requires a

---

Investigatory Powers Act 2000, c. 23, § 5 (U.K.), http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf. The FRA Report identifies five Member States that engage in the collection of signals intelligence (collection that, at least in the initial stage, targets large flows of data and not an individual). None of these Member States – France, Germany, the Netherlands, Sweden, and the United Kingdom – has a judicial body involved in the approval of signal intelligence. FRA Report at 55, Table 5.

[12] Peter Swire, Justin Hemmings & Suzanne Vergnolle, *Mutual Legal Assistance Case Study: The United States and France*, WISC. INT'L L.J. (forthcoming 2016) [hereinafter *Mutual Legal Assistance Case Study*].

[13] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

[14] In this context, the search is considered to be reasonable if the law enforcement obtained a valid warrant before the search was conducted. DANIEL J. SOLOVE & PAUL SWARTZ, INFORMATION PRIVACY LAW (4th ed. 2015).

[15] *Brinegar v. United States*, 338 U.S. 160 (1949). U.S. Supreme Court cases may be found at https://www.supremecourt.gov/opinions/opinions.aspx or https://supreme.justia.com/.

[16] *Horton v. California*, 496 U.S. 128 (1990). *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.

heightened standard of proof. Wiretaps are understood as requiring "probable cause plus," with requirements before the courts permit real-time interception:

1. An interception order requires "a particular description" of both the "nature and location of the facilities from which or the place where the communication is to be intercepted" and "the type of communications sought."[17]

2. The application for an interception order must explain "whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or be too dangerous."[18] Failure to exhaust alternate, less-intrusive means of obtaining the same information can result in the denial of an application for an interception order.[19]

3. The application must specify the period of time during which the interception will take place, or a reason why the applicant has probable cause to believe no termination date should be set because additional covered communications will continue to occur.[20] Minimization rules apply so non-relevant communications are not authorized by the wiretap.[21]

4. There are multiple rounds of review within the Department of Justice before a wiretap request can go to a judge – magistrates on their own motion cannot approve a wiretap.[22]

[13] The judge must make a determination in favor of the government on all of these factors to issue an order permitting the interception.[23] Once the order is approved, the government is responsible for complying with minimization procedures. Specifically, the order is to be executed as soon as possible, is to be conducted in such a way as to minimize the incidental collection of communications not subject to the order, and is to be terminated once the communication authorized under the order is obtained.[24] Within 90 days of the termination of the order, the individual who was searched must be notified by the court of the existence of the order.[25]

---

[17] 18 U.S.C. § 2518(1)(b).
[18] *Id.* § 2518(1)(c).
[19] *Id.*
[20] *Id.* § 2518(1)(d).
[21] *Id.* § 2518(5); *see, e.g.*, *United States v. Rivera*, 527 F.3d 891, 904-05 (9th Cir. 2008), https://casetext.com/case/us-v-rivera-33 (describing the government's minimization efforts).
[22] 18 U.S.C. § 2518(1); *see also* 18 U.S.C. § 2510(9) (defining an approving judge as "(a) a judge of a United States district court or a United States court of appeals, and (b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications").
[23] *Id.* § 2518(3). If the request is denied, the court must notify the individual who was the target of the request within 90 days of the denial. *Id.* § 2518(8)(d).
[24] *Id.* § 2518(6).
[25] *Id.* § 2518(8)(d).

D. The Exclusionary Rule, Preventing Prosecutors' Use of Evidence that Was Illegally Obtained, and Civil Suits

[14] In the US criminal law area, individual remedies exist to address evidence obtained during a search that was illegally conducted. In a criminal trial in the US, the courts enforce constitutional rights by excluding evidence that the government obtains illegally.[26] In addition, the courts bar evidence that is "the fruit of a poisonous tree" – additional evidence similarly cannot be used in court if it is derived from an illegal search.[27] Since the 1960s, this "exclusionary rule" has served as an important practical motivation for police officers to follow the rules for searches and seizures.

[15] With regard to civil remedies, an individual who has been the subject of a search that violated the Fourth Amendment can file a lawsuit seeking monetary damages.[28] When the law enforcement officials conducting the search are state or local employees, the individual files a civil rights suit pursuant to 42 U.S.C. § 1983.[29] In a Section 1983 claim, the plaintiff can recover compensatory damages and reasonable attorney's fees. The courts have permitted suits by US citizens and non-US citizens living in the US. [30] In short, the US exclusionary rule, backed up by the "fruit of the poisonous tree" doctrine and civil remedies, provides clear individual remedies against illegal searches.

[16] The adversarial system in the US makes this remedy quite different than the laws in many European countries. For example, in the French system, a search only needs to be necessary to establish the "truth," and any evidence "necessary to establish the truth" can be presented to the bodies investigating and ultimately prosecuting the crime.[31]

E. Other Legal Standards that are Relatively Strict for Government Access in Many Non-Search Situations, such as the Judge-Supervised "Reasonable and Articulable Suspicion" Standard under ECPA

[17] Under the Electronic Communications Privacy Act (ECPA), categories of information that do not require probable cause have historically been available to the government when a judge is

---

[26] *Mapp v. Ohio*, 367 U.S. 643 (1961). In addition to exclusion from evidence under the Fourth Amendment, certain statutes, such as the Wiretap Act, provide for exclusion of evidence for violation of the statutory requirements. *See* 18 U.S.C. § 2518(10)(a).

[27] *Wong Sun v. U.S.*, 371 U.S. 471 (1963).

[28] SOLOVE & SWARTZ, *supra* note 14; *see* 18 U.S.C. § 2518(10)(a).

[29] In addition to § 1983 claims, certain federal statutes provide for a basis for a civil suit. *See* 18 U.S.C. § 2511(4)(a); 18 U.S.C. § 2701(b).

[30] Under § 1983, an aggrieved person is "any citizen of the United States or other person within the jurisdiction thereof." 42 U.S.C. §1983; *see also Plyler v. Doe*, 457 U.S. 202 (1982); *Graham v. Richardson*, 403 U.S. 365 (1971); Martin Schwartz, *Section 1983 Litigation*, FEDERAL JUDICIAL CENTER 27 (2014), https://www.casd.uscourts.gov/Attorneys/CJAAppointments/SiteAssets/docs/FJCSection1983Outline.pdf [hereinafter *Section 1983 Litigation*]. Because Section 1983 claims do not extend to instances where the law enforcement officials conducting the search were federal officers, the United States Supreme Court has recognized an implied remedy known as a *Bivens* claim, so named for the 1971 case in which the claim was first discussed. *See Bivens v. Six Unknown Agents*, 403 U.S. 388 (1971). Generally, the same legal principles and procedures apply in a *Bivens* claim as in a § 1983 claim. *Id.*

[31] For a full comparison of these concepts in French and US laws, *see Mutual Legal Assistance Case Study*.

satisfied that reasonable suspicion exists to believe that the data is relevant to an ongoing criminal investigation based on "specific and articulable facts" presented by the government.[32] This requirement of reasonable and articulable suspicion means that the government must meet the touchstone of the Fourth Amendment's requirement for reasonableness, but does not require a search warrant because the level of intrusion is considered lower than that in a full search.[33]

[18] More recently, federal appellate courts have interpreted ECPA to say that requests under Section 2703(b) (content of communications) do require a probable cause warrant.[34] Some magistrates have placed even further limitations on obtaining content, such as the length of time the content can be retained and limits on searching within a computer for all the files in that computer.[35]

[19] Compared with the approaches in France and other EU countries, the analysis is similar to that provided for the probable cause standard. Once again, an independent judge in the US must make the decision whether the legal standard has been met for the government to access the evidence.

F. Transparency Requirements, such as Notice to the Service Provider of the Legal Basis for a Request

[20] US law and practice is to have clear notice in the judge's order to produce evidence of the legal basis for the order, for instance by citing the specific statutory provision under which the order is issued.[36] This notice enables the recipient of the order to research the lawful basis, to help determine whether there are reasons to challenge the order. By contrast, it is my understanding that companies that receive requests for electronic evidence in many EU and other jurisdictions lack this information about the legal basis for the evidence request.

---

[32] 18 U.S.C. § 2703(d).

[33] The standard derives from *Terry v. Ohio*, 392 U.S. 1 (1968), which established the reasonable and articulable suspicion test for brief police stops of individuals. For one discussion of the relative role of *Terry*, probable cause, and other standards, *see* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 21–47 (2007).

[34] *See e.g., United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), http://www.opn.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf (holding the Fourth Amendment prevents law enforcement from obtaining stored email communications without a warrant based on probable cause); *United States v. Ali*, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012), https://casetext.com/case/united-states-v-ali-5 ("[I]ndividuals have a reasonable expectation of privacy in the content of emails stored, sent, or received through a commercial internet service provider.").

[35] *See United States v. Ganias*, 755 F.3d 125, 134 (2d Cir. 2014), https://casetext.com/case/united-states-v-ganias ("Because the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge is to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools."); *see also Matter of Black iPhone 4*, 27 F. Supp. 3d 74, 78 (D.D.C. 2014), https://casetext.com/case/in-re-in-re-iphone (holding the government "must be more discriminating when determining what it wishes to seize, and it must make clear that it intends to seize *only* the records and content that are enumerated and relevant to its present investigation").

[36] 18 U.S.C. § 2703(b).

G. Lack of Data Retention Rules for Internet Communications

[21] Data retention requirements have been a prominent feature of European debates about how to achieve privacy protections consistent with law enforcement and national security goals. In 2006, the EU promulgated a Data Retention Directive, which required publicly available electronic communications services to retain records for an extended period of time, for purposes of fighting serious crime.[37] For instance, for email and other electronic communications, the communications services were required to retain "the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication."[38] In the *Digital Rights Ireland* case, the European Court of Justice struck down that Directive due to privacy concerns related to excessive access to the retained data and lack of assurances that the records would be destroyed at the end of the retention period.[39] In the wake of that judgment, a number of EU Member States have reinstated modified data retention requirements for telephone and Internet communications.[40]

[22] By contrast, the US does not require data retention for email or other Internet communications. Internet data retention bills have been introduced in Congress, but have not come close to passage.[41] The Federal Communications Commission has issued rules concerning retention of telephone records for up to 18 months.[42] Those rules apply only to "telephone toll records," which are a diminishing portion of all communications, as users increasingly rely on non-telephone Internet communications and often have unlimited phone calls, so toll records are no longer required for billing purposes.

[23] In light of the significant privacy concerns explained in the *Digital Rights Ireland* case, the presence of data retention rules in the EU and their general absence in the US support the view that the absence of such rules is a significant check on the power of government in both law enforcement and foreign intelligence investigations.

H. Lack of Limits on Use of Strong Encryption

[24] At the time of this writing in October 2016, there have been calls for new limits on strong encryption in a growing number of EU countries, including a joint press conference by the

---

[37] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, O.J. (L 105) 54, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

[38] *Id.* at Art. 5(1)(b).

[39] C-293/12, *Digital Rights Ireland v. Minister of Commc'ns*, 2014 E.C.R. I-238, http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN.

[40] Federico Fabrinni, *Human Rights in the Digital Age: The European Court of Justice Ruling in Digital Rights Ireland and its Lessons for Privacy and Surveillance in the U.S.*, 28 HARV. HUM. RTS J. 65 (2015), http://harvardhrj.com/wp-content/uploads/2009/09/human-rights-in-the-digital-age.pdf.

[41] *See* CENTER FOR DEMOCRACY & TECHNOLOGY, *Resources on Data Retention* (Sept. 26, 2012), https://cdt.org/insight/resources-on-data-retention.

[42] 47 C.F.R. § 42.6.

Interior Ministers of France and Germany.[43] In the United Kingdom, in addition to relatively strict rules relating to encryption in the Regulation of Investigatory Powers Act of 2000,[44] limits on end-to-end encryption are included in the proposed Investigatory Powers Bill, which has passed most of the hurdles to passage.[45] In my view and the view of many other experts, such limits on the use of strong encryption pose serious threats to user privacy.[46]

[25] Debates about the use of strong encryption have also occurred recently in the US, most prominently expressed by FBI Director James Comey in the controversy about encryption of the Apple iPhone.[47] The US historically permitted use of strong encryption within the country but limited exports of strong encryption through export control laws. The bulk of these export controls were eliminated in 1999.[48] Based on my extensive experience with encryption policy in the US, I believe legislation limiting the use of strong encryption has a low likelihood of passage.[49] Meanwhile, a number of EU Member States retain stricter laws governing encryption than the US, including France and Hungary.[50] Indeed, US-based technology companies have taken a global position of leadership on use of strong encryption, bolstering the likelihood that encryption-enabled privacy protections will continue to develop in the US.

III. Conclusion

[26] Based on my academic research and other experience, it is a complex task to assess precisely where the US and EU provide stricter safeguards concerning government criminal investigations. This Chapter seeks to inform the more general question of whether the US has "adequate" or "essentially equivalent" safeguards to the Member States of the EU for government access to information about a defendant or other data subject.

---

[43] Natasha Lomas, *Encryption under fire in Europe as France and Germany call for decrypt law*, TECHCRUNCH, (Aug. 24, 2016) https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-france-and-germany-call-for-decrypt-law/.

[44] *See* Bert-Jaap Koops, *Crypto Law Survey, Overview per country, Version 27.0*, CRYPTOLAW.ORG (Feb. 2013) http://www.cryptolaw.org/cls2.htm.

[45] Tirath Bansal, *Investigatory Powers Bill: Rushed through under Cover of Brexit*, COMPUTERWEEKLY.COM (July 13, 2016), http://www.computerweekly.com/news/450300206/Investigatory-Powers-Bill-rushed-through-under-cover-of-Brexit.

[46] *See, e.g.*, *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy Before the S. Comm. on the Judiciary*, 114th Cong. (2015) (statement of Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business Georgia Institute of Technology), https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf; Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by requiring government access to all data and communications*, MIT COMP. SCI. AND ARTIF. INTEL. LAB. (July 6, 2015), http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

[47] Lev Grossman, *Inside Apple CEO Tim Cook's Fight with the FBI*, TIME MAG. (Mar. 17, 2016), http://time.com/4262480/tim-cook-apple-fbi-2/.

[48] Press Briefing by Deputy National Security Advisor Jim Steinberg, Attorney General Janet Reno, Deputy Secretary of Defense John Hamre, Under Secretary of Commerce Bill Reinsch, and Chief Counselor for Privacy at OMB Peter Swire, WHITE HOUSE, OFFICE OF THE PRESS SEC'Y (Sept. 16, 1999), http://www.peterswire.net/archive/privarchives/Press%20briefing%20Sept.%2016%201999.html.

[49] Swire in 1999 chaired the White House Working Group on Encryption when the US repealed most of the export controls on export of strong encryption. Since then, Swire has written extensively on encryption law and policy. *See, e.g.*, Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416 (2012), http://stlr.org/volumes/volume-xiii-2011-2012/encryption-and-globalization/.

[50] *See* Bert-Jaap Koops, s*upra* note 44.

[27] The Chapter has described how the creation of the US itself derived in significant measure from an insistence on protecting the rights of individuals in the criminal justice system. That tradition of the Bill of Rights remains in effect today.

[28] The Chapter has also documented eight ways in which the US usually or generally has stricter protections than EU Member States. In the Emory Law Journal article, we call these eight "plus factors," ways that an assessment of the US system should provide additional points – "plus factors" – compared to the EU approach. Critics of the US approach have sometimes listed specific safeguards that exist in an EU country but not in the US and have found these missing pieces to be relevant to an overall assessment of "adequacy" or "essential equivalence." My point here is that the US has significant, and often constitutional, safeguards that usually are lacking in the EU. In my view, a fair comparison of the adequacy of the two systems should carefully consider such additional factors.