International Conflict of Law: Online Aspects, Part Three - Substantive Issues

Prepared by:
Bob Ellis
Hennis, Rothstein & Ellis LLP

LORMAN®

Published on www.lorman.com - July 2020

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 110+ live webinars added every month
- ☑ **Unlimited OnDemands** - Over 3,900 courses available
- ☑ **Videos** - More than 1,900 available
- ☑ **Slide Decks** - More than 3,300 available
- ☑ **White Papers** - More than 2,000 available
- ☑ **Reports**
- ☑ **Articles**
- ☑ **... and much more!**

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: **www.lorman.com/pass/?s=special20**

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Substantive Issues

(1) *Outbound: Extraterritorial Applicability of American Substantive Law*

Although in an online context, the United States does not normally claim that its laws apply extraterritorially, it does have the power to do so, subject to four guiding principles:

- First, the *territorial principle,* under which "[a]bsent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application."[107] Congress did clearly express such an intent regarding a few statutes, among them the Foreign Corrupt Practices Act,[108] the Wire Act,[109] the Wire Fraud Act,[110] the Computer Fraud and Abuse Act,[111] and many visa and immigration laws.[112] The Electronic Communications

---

[105] *Id.*, ¶¶ 132-133.

[106] Equustek Solutions Inc. v. Google, Inc., 2-15 BCCA 265 (Court of Appeal for British Columbia June 11, 2015): Where "the most important facts on which the injunction application is based–facts concerning the violation of trade secrets and of intellectual property rights–have a strong connection with the Province" (*id.* ¶ 41) and where "Google's services, which provide a link between the defendant's products and potential customers, are substantially connected to the substance of the lawsuit," (*id.* ¶ 51), jurisdiction was proper. The court disregarded Google's choice-of law and forum selection clauses: "Although those contracts stipulate that disputes will be governed by California law and adjudicated in California courts, the 'choice of laws' provision in those contracts does not alter the fact that Google is carrying on a business in this province. . . ." (*id.* ¶ 52, quoting other authority).

[107] RJR Nabisco, Inc. v. European Community, 579 U.S. __, 136 S.Ct. 2090, 2093, 195 L.Ed.2d 476 (2016). See also:
Supreme Court: Bond v. United States, 572 U.S. 844, 134 S.Ct. 2077, 2088, 189 L.Ed.2d 1 (2014) ("[W]e presume, absent a clear statement from Congress, that federal statutes do not apply outside the United States."); Kiobel v. Royal Dutch Petroleum Co., 569 U.S. ___, 133 S.Ct. 1659, 185 L.Ed.2d 671 (2013) (presumption against extraterritoriality applies to the Alien Tort Statute, 28 U.S.C. § 1350); Morrison v. National Australia Bank Ltd., 561 U.S. 247, 255, 130 S.Ct. 2869, 177 L.Ed.2d 535 (2010).
Second Circuit: Matter of Warrant to Search a Certain E–Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016); United States v. Yousef, 327 F.3d 56, 86 (2d Cir. 2003) (citing Foley Brothers v. Filardo, 336 U.S. 281, 285, 69 S.Ct. 575, 93 L.Ed. 680 (1949)).
Ninth Circuit: Subafilms, Ltd. v. MGM-Pathe Communications Co., 24 F.3d 1088 (1994) (federal copyright law does not have extraterritorial effect).

[108] 14 U.S.C. §§ 78dd2 and 78dd3.

[109] A federal law, "unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States. . . . The Wire Act expresses such a contrary intent because it explicitly applies to transmissions between the United States and a foreign country." United States v. Lyons, 740 F.3d 702 (1st Cir. 2014) (citing 18 U.S.C. § 1084).

[110] 15 U.S.C. § 1343. See United States v. Georgiou, 777 F.3d 125 (3d Cir. 2015).

[111] A "protected computer . . . includ[es] a computer located outside the United States that is used in a manner that affects interstate or foreign commerce." 18 U.S.C. § 1030(e)(2)(B). See WesternGeco LLC v. ION Geophysical Corp., __ U.S. __, 138 S.Ct. 2129, 2136, 201 L.Ed.2d 584,___ (2018): "This Court has established a two-step framework for deciding questions of extraterritoriality. The first step asks 'whether the presumption against extraterritoriality has been rebutted.' It can be rebutted only if the text provides a 'clear indication of an extraterritorial application.' If the presumption against extraterritoriality has not been rebutted, the second step of our framework asks 'whether the case involves a domestic application of the statute.' Courts make this determination by identifying 'the statute's "focus"' and asking whether the conduct relevant to that focus occurred in United States territory. If it did, then the case involves a permissible domestic application of the statute."

[112] United States v. Pizzarusso, 388 F.2d 8,9 (2d Cir. 1968) (Regarding defendant's claim that the law criminalizing the making of false statements on a visa did not apply to her conduct outside the U.S.: "In the ordinary course of events we would naturally expect false statements in visa applications to be made outside the territorial limits of the United States. This would seem to overcome the strong presumption that the Congress did not intend the statute to apply extraterritorially.").

Privacy Act has been held to protect non-U.S. citizens located outside the U.S. when they use e-mail communications provided by U.S.-based e-mail providers.[113] Intellectual property laws such as the Copyright Act[114] and the Lanham (trademark) Act[115] do not apply extraterritorially, so pursuit of infringements in a foreign country must be based either on a treaty or on the law of the country in which the infringement occurs. Similarly, neither the Wiretap Act[116] nor the Communications Decency Act[117] applies extraterritorially.

- Second, the *nationality principle*, which "permits a nation to extend its legislative jurisdiction—or "jurisdiction to prescribe"—to cover the conduct of its nationals abroad, is among the most firmly established bases for jurisdiction recognized by international law."[118] The nationality principle has been invoked almost exclusively in criminal cases.

- Third, the *protective principle*, under which a nation can regulate conduct outside its territory that threatens its security or the operation of its governmental functions.[119]

- Fourth, the *principle of respect for the law of nations.* "It has been a maxim of statutory construction since [1804] that 'an act of congress ought never to be construed to violate the law of nations, if any other possible construction remains. . . .'"[120]

---

[113] In 2012, the Ninth Circuit ruled that the ECPA's language in 18 U.S.C. § 2702(a)(1) that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service" applies to entities within the U.S., no matter where the account holder is located, and ordered the quashing of a subpoena seeking the e-mails of a citizen of India who was located in India. Suzlon Energy Ltd. v. Microsoft Corp., 2011 WL 4537843 (9th Cir. Oct. 3, 2011).

[114] *Ninth Circuit:* Subafilms, Ltd. v. MGM-Pathe Communications Co., 24 F.3d 1088, 1096 (9th Cir. 1994) (U.S. copyright law has "no application to extraterritorial infringement.") The same is true in other countries, of course. See, e.g., Paramount Home Entertainment International Ltd v. British Sky Broadcasting Ltd [2013] EWHC 3479 (Ch) (England and Wales High Court of Justice found that certain U.S. websites that had been providing links accessing material that had been found to be infringing under U.K. law. Rather than attempting to apply U.K. law extraterritorially, the High Court issued orders requiring ISPs within the U.K. to block access to those sites).
Eleventh Circuit: Dish Network LLC v. TV Net Solutions, LLC, 2014 WL 6685366 (M.D. Fla. Oct. 10, 2014) (injunction directed at foreign country would exceed the territorial scope of the Copyright Act).

[115] Trader Joe's Company v. Hallatt, 981 F. Supp.2d 972 (W.D. Wash. 2013).

[116] In Doe v. Federal Democratic Republic of Ethiopia, 189 F. Supp.3d 6, 15 (D.D.C. 2016), *aff'd* No. 16-7081, 2017 WL 971831 (D.C. Cir. March 14, 2017), a citizen whose online activities had apparently been spied on by Ethiopia sued that government for violating the Wiretap Act. The court held that "the Wiretap does not create a civil cause of action against a foreign state for interceptions of wire, oral, or electronic communications in violation of section 2511(1)."

[117] In Cohen v. Facebook, Inc., 252 F. Supp. 3d 140, 159 (E.D.N.Y. 2017), aff'd in part, dismissed in part sub nom. Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019), and aff'd in part, dismissed in part sub nom. Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019), the plaintiff argued that since the CDA did not contain any indication of extraterritorial applicability, then, pursuant to the territorial principle, the statute, in particular Section 230, its immunity provision, could not be applied to immunize alleged conduct (knowingly allowing terrorists to use its social networking service to plan and coordinate terrorist attacks) that occurred outside the United States. The court, noting that "[n]o other court appears to have addressed the presumption against extraterritoriality in the context of a statute which limits liability or imparts immunity," held that Section 230 simply states that an online provider is not to be treated as the publisher or speaker of any third party content, without regard to the location of the third party content. "In light of its focus on limiting civil liability, the court concludes that the relevant location is that where the grant of immunity is applied, i.e., the situs of the litigation." *Id.*, at *15.

[118] United States v. Pizzarusso, 388 F.2d 8,10 (2d Cir. 1968).

[119] *Id.*, 388 F.2d 8.

[120] Weinberger v. Rossi, 456 U.S. 25, 32, 102 S.Ct. 1510, 1516, 71 L.Ed.2d 715 (1982) (quoting Murray v. Schooner Charming Betsy, 2 Cranch 64 (1804)). With respect to foreign sovereigns, the Foreign Sovereign Immunities Act (FSIA), 28 U.S.C. § 1602, legislatively establishes an important aspect of the principle of respect for the law of nations, providing that American courts have no jurisdiction to hear claims against foreign states. See, e.g., Democratic Nat'l Comm. v. Russian Federation, 392

Extraterritorial application of United States substantive law regarding the Internet has never been much of an issue, in large part because Congress and the courts have consistently respected these four principles in enacting and construing U.S. law. The same cannot be said regarding attempts by other nations to apply their substantive law to persons within the United States.

(2) *Inbound: Applying Foreign Substantive Law to Persons Within the United States*

In an online context, the most frequent instances of foreign governments and courts claiming that their laws and rulings apply within the United States involve attempts to suppress the availability of information, and attempts to prevent American companies from collecting or using information about persons located outside the United States. Sometimes the information in question is supposedly defamatory, sometimes it is claimed to violate privacy or consumer rights, and sometimes it is claimed to be seditious.

[i]—Suppression of Online Information

Back when the world was not online, it was relatively simple for governments, especially authoritarian ones, to suppress the dissemination of ideas. "This was a world in which photocopiers were banned. There were typewriters but even these were registered and numbered. Both the typewriter and the photocopier were instruments of potential societal discord and instruments which could create a challenge to the regime."[121] With the advent of the Internet, the ability of authorities to restrict the dissemination of ideas by restricting photocopy machines[122] and confiscating printed materials disappeared forever.[123] Instead, virtually all efforts at suppression shifted to the Internet. Many governments throughout the world engage in activities that can be characterized as attempts to control, suppress, and otherwise restrict the Internet: Spying on those who

---

F.Supp.3d 410, 418 (S.D.N.Y. 2019): "The primary wrongdoer in this alleged criminal enterprise is undoubtably the Russian Federation, the . . . entity that surreptitiously and illegally hacked into the DNC's computers and thereafter disseminated the results of its theft. But . . . under the Foreign Sovereign Immunities Act . . . , the Russian Federation cannot be sued in the courts of the United States for governmental actions, subject to certain limited exceptions not present in this case, just as the United States government generally cannot be sued in courts abroad for its actions. The remedies for hostile actions by foreign governments are state actions, including sanctions imposed by the executive and legislative branches of government." FSIA does, however, contain a "commercial activity exception" similar to those in domestic sovereign immunity statutes, as well as an expropriation exception. In Cassirer v. Kingdom of Spain, 616 F.3d 1019 (9th Cir. 2010), which addressed both exceptions, the court found that a website run by the government of Spain was a factor in its finding that Spain engaged in sufficient commercial activity within the U.S. to meet that exception. Another aspect of the principle of respect for the law of nations is the "Act of State Doctrine," which bars a court from exercising authority over a foreign sovereign even when one of the FSIA exceptions applies. The Act of State Doctrine applies when "(1) there is an official act of a foreign sovereign performed within its own territory; and (2) the relief sought or the defense interposed in the action would require a court in the United States to declare invalid the foreign sovereign's official act." Sea Breeze Salt, Inc. v. Mitsubishi Corp., No. CV162345, 2016 WL 8648638 at *3 (C.D. Cal. Aug. 18, 2016) (dismissing a commercial case against a company owned 51% by the government of Mexico, where the acts complained of took place in Mexico).

[121] Gillies, "Information Futures," Australian Library J. (Nov. 2002), § 51:4, 339-352, available at http://dx.doi.org/10.1080/00049670.2002.10756005.

[122] "In Czechoslovakia, for example, where there are a mere 8,000 copiers for 15 million people, most machines are in government offices and state-owned companies, where their use is strictly controlled. 'When you wanted to make a copy of something, you had to have a signed form for a definite number of copies.' . . . At the state-owned copying center in Prague, lines were long and the authorities monitored customers." Prokesch, "The Challenge of Marketing: Xerox tackles Eastern Europe," Ocala (Florida) Star-Banner, p. 6F (Dec. 27, 1990).

[123] See Kalathil and Boas, "Open Networks–Closed Regimes: The Impact of the Internet on Authoritarian Rule," Carnegie Endowment for International Peace, 2003.

use the Internet by monitoring and archiving all Internet traffic,[124] blocking access to certain sites or services,[125] requiring all operators of online forums to register,[126] broadly expanding the definition of, and penalties for, defamation, treason, and the like,[127] criminalizing some (even mild) expressions or images as "violating public

---

[124] The scope of NSA surveillance revealed by the Snowden revelations surprised even security experts, but even at that time many countries throughout the world had engaged in online surveillance for years. In 2000, then-interim Russian president Putin issued what may have been the first publicly acknowledged regulation in this regard, a provision allowing the FSB, the KGB's successor, to be hard-wired into each of Russia's ISPs so as to have real-time access to all Internet traffic. Ministry of Communications of Russia, 25.07.2000 No. 130 "On the order of leveraging technology to provide search operations on the telephone networks, mobile and wireless communications, and personal radio public." (Russian Internet and wiretap laws are grouped under the Russian acronym COPM or SORM.) That same year, the U.K. followed the KGB's example but added even more invasive provisions by enacting the Regulation of Investigatory Powers Act 2000, which requires all ISPs in the U.K. to route a copy of all data passing through their systems to MI5, the British secret police. Under the act, all subjects in the U.K. must surrender all passwords and decryption codes whenever a public authority demands them, and if the code belongs to a private company, the individual may not reveal to the company that the codes have been compromised. Public Acts of the U.K. Parliament 2000, Ch. 23., available at www.legislation.gov.uk/ukpga/2000/23/contents. Commentary can be found in *Infoworld*, p. 28 (Sept. 4, 2000). In 2001, of course, the USA Patriot Act was enacted, enabling unprecedented new levels of NSA surveillance.

[125] China, for example, blocks access to Twitter, virtually all of Google, Facebook, Snapchat, YouTube, and thousands of websites. When, in 2014, China imposed even tighter restrictions on e-mail, "[b]usiness travelers complained they will no longer be able to access email while in China without jumping through hoops. Their Chinese counterparts complained that it will now be more difficult to conduct business internationally. . . . Taken together, the restrictions constitute the world's largest–and most effective–state-sponsored censorship program." Riley, "The Great Firewall of China Is Nearly Complete," CNN/Money (Hong Kong) (Dec. 30, 2014), available at http://money.cnn.com/2014/12/30/technology/china-internet-firewall-google/. Turkey threatened to block Twitter as well, citing violations of national security laws: Arsu, "Turkey Threatens to Block Social Media over Released Documents," New York Times (Jan. 16, 2015), available at http://nyti.ms/1KRBMzw. Russia routinely blocks sites and other communications deemed a threat to public order, which is interpreted to include opposition rallies. Khrennikov and Ustinova, "Google Warning on Russia Prescient as Putin Squeezes Web," BloombergBusiness (April 30, 2014), available at http://www.bloomberg.com/news/articles/2014-04-29/google-warning-on-russia-prescient-as-putin-squeezes-web. In 2007, a São Paulo court ordered a Brazilian online service provider as well as phone companies to block all access to YouTube as long as a video showing two celebrities having sex was still available. Reported by Haines, "Brazil's ISPs stuff YouTube," The Register (UK) (Jan. 9, 2007), available at www.theregister.co.uk/2007/01/09/youtube_waxed/). In 2014, Turkey attempted to replace foreign DNS servers with its own in an attempt to control and suppress social networks and other sites. Mirani, "Turkey's Increasingly Troubling Efforts to Control the Internet," Nextgov.gov (March 31, 2014), available at www.nextgov.com/cio-briefing/2014/03/turkeys-increasingly-troubling-efforts-control-internet/81598/. Also in Turkey, in 2015, a court ordered that Facebook pages that insult the prophet Muhammad be blocked within the country, and in another ruling ordered that all access in Turkey to web pages depicting the French satirical cartoon journal Charlie Hebdo be blocked. "Turkish court orders Facebook pages blocked," Phys.org (Jan. 26, 2015), available at http://phys.org/news/2015-01-turkish-court-facebook-pages-blocked.html. In 2017 Russia blocked all access to LinkedIn and prohibited downloads of the LinkedIn app. Reported in numerous sources, e.g., Kang and Benner, "Russia Requires Apple and Google to Remove LinkedIn From Local App Stores," New York Times (Jan. 6, 2017), available at http://nyti.ms/2i242YQ.

[126] In 2014, Russian President Putin signed into effect the so-called "Bloggers' Law," a statute requiring any website with more than 3,000 daily visitors to be liable for any inaccuracy posted on their forum. Bloggers cannot be anonymous. Russian Federation, Law No. 97-FZ (May 5, 2014), "On Amendments to the Federal Law."

[127] One example from Britain: A U.K. trial court ruled that *A Piece of Blue Sky*, a book critical of Scientology, was defamatory and issued an injunction prohibiting distribution. Amazon removed the book from its website when it was informed of the injunction. This resulted in a firestorm of criticism in the U.S., in reaction to which Amazon returned the book to its website but refused to sell it to U.K. addresses. Reported in IP Worldwide (Aug.-Sept. 2000), p. 18. See also, Chidi, "Web Law Blocks Growth," Infoworld, p. 37 (March 5, 2001). Another example from Russia:

> "In July 2012, defamation was reintroduced as a criminal offence in Russia, which mandates fines on media outlets of up to two million rubles (approximately $61,000) for producing 'defamatory' public statements. Also in July 2012, changes introduced to the Law on 'Information, Information Technologies and Information Protection' increased Internet censorship and curbed the freedom of expression. On October 23, 2012, the law on amendments to the criminal code was adopted, which expands the definition of treason, making it so vague as to enable the government to brand a critic as a traitor."

International Center for Not-for-Profit Law, NGO Law Monitor: Russia (Nov. 2014), available at http://www.icnl.org/research/monitor/russia.html.

decency"[128] or as "hate speech,"[129] or banning specific websites, images, files, or videos.[130] Most western democracies, including the United States, are to some extent involved in similar efforts as well.[131] Indeed, there is general agreement in virtually all countries that some restrictions and content suppression are justifiable, child pornography being one example, but once the principle is established that some suppression is appropriate, questions arise: what content should be suppressed, what country's laws should apply, and who decides?

For decades, most governmental efforts to censor or control online content were national in scope. China's "Great Firewall" comes to mind. It was rare for a country to claim that its laws applied outside its own territory. There were, however a few early signs of what was to come.

[A]—The German CompuServe Prosecution

In an early case challenging the limits of extraterritoriality, Germany—which at the time (1998) claimed that its laws regarding what is forbidden on the Internet in

---

[128] Alleged public decency violations online are a frequent basis for prosecution and worse in many Middle Eastern countries. In 2013, three teenagers were put on trial in Morocco for posting Facebook photos of two of them kissing. Press report, "Teenage couple's kiss shakes Morocco by Internet effect, triggers calls for kiss-ins," Hurriet Daily News (Turkey) (Oct. 12, 2013), available at www.hurriyetdailynews.com/teenage-couples-kiss-shakes-morocco-by-internet-effect-triggers-calls-for-kiss-ins-.aspx?pageID=238&nID=56142&NewsCatID=357.

[129] In the U.K., "ISPs have begun implementing the mandatory porn filtering that Prime Minister David Cameron has been pushing, and the results are about what you'd expect: all sorts of non-pornographic sites are being blocked, including important sex education sites and, more troubling, rape and sexual abuse information sites (while plenty of porn is getting through)." Masnick, "ISP Blocks For Copyright And Porn Denying Access To All Sorts Of Important Information," Techdirt (Dec. 20, 2013), available at https://www.techdirt.com/articles/20131219/11532825635/isp-blocks-copyright-porn-denying-access-to-all-sorts-important-information.shtml.

[130] Although not an example of an "outbound" jurisdictional claim, in 2013, the U.S. State Department demanded that a website operator remove online blueprints for a 3D-printable handgun as well as blueprints for other printable firearms components, pending a review of the site's compliance with export control laws. Greenberg, "State Department Demands Takedown Of 3D-Printable Gun Files For Possible Export Control Violations," Forbes (May 9, 2013), available at http://www.forbes.com/sites/andygreenberg/2013/05/09/state-department-demands-takedown-of-3d-printable-gun-for-possible-export-control-violation/. In 2013 courts in Brazil imposed fines on Facebook and Google for refusing to block or remove certain photos from sites they host. Parkinson, "Facebook and Google fined by Brazilian court over 'morbid images.'" Guardian (July 9, 2015), available at http://www.theguardian.com/technology/2015/jul/09/facebook-google-fined-brazilian-court-morbid-images. There are many other examples. Many online sites have started tracking and reporting the number of government requests to block or remove information, including statistics regarding the reasons cited for removal. See, e.g., Google Transparency Report/Government Removals, www.google.com/transparencyreport/removals/government/?hl=en. In addition to removal requests, a number of governments simply block certain sites or portions of them. For example, in early 2014, Malaysia suddenly began blocking a number of American websites that displayed user-posted photos, some of which were racy. Since Malaysia did not have a history of doing this, the companies inquired discreetly with law enforcement offices in Malaysia, and were told to be patient, that the blocking was political, and that the sites would be unblocked after the election—a prediction that turned out to be correct. (Personal experience of author.)

[131] See, e.g., "More governments are shutting down the Internet. The harm is far-reaching.) Washington Post (editorial), Sept. 7, 2019. In 2014, the Center for Internet and Society at Stanford University released a World Intermediary Liability Map (WILMAP), a detailed and continuously updated country-by-country compilation of laws, proposed laws, and court decisions from around the world related to freedom of expression and user rights. http://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap. Another similar country-by-country study is Freedom House, "Freedom on the Net 2014" (updated annually with corresponding year changes), available at https://freedomhouse.org/report/freedom-net/freedom-net-2014. Also useful in this context is Bitso, Fourie and Bothma, "Trends in transition from classical censorship to Internet censorship: selected country overviews" (International Federation of Library Associations (Oct. 5, 2012), available at http://www.ifla.org/publications/trends-in-transition-from-classical-censorship-to-intenet-censorship-selected-country-o.

Germany had worldwide applicability[132]—convicted the executive director of CompuServe's German subsidiary for violating Germany's obscenity laws because U.S.-based CompuServe, an online service provider, failed to block access to material on its servers in Ohio that was illegal in Germany.[133] The indictment quickly became an embarrassment for the prosecution, which changed its mind during the trial and argued against conviction. CompuServe's response was to pull all its offices out of Germany.[134]

[B]—British Obscenity Case

In another early case, a British court held that the content of an American pornographic website was subject to British law and was in violation of Britain's Obscene Publications Act.[135]

[C]—The Yahoo France Case

A seminal case addressing substantive extraterritoriality arose in France in 2000. A French advocacy group demanded that Yahoo remove all Nazi-related discussions and all depictions of Nazi artifacts from its auction site since such auctions and related discussions were illegal under French law. In response, Yahoo removed all such items from its yahoo.fr website, but refused to remove them from its U.S. site. The advocacy group, not satisfied, sued, even though the offending pages were posted on Yahoo's U.S. site, in English, by U.S. citizens, and the auctions were not only legal in the U.S., but were protected by the First Amendment. A Paris court, apparently unimpressed with the First Amendment, ordered[136] Yahoo to remove the offending items from its U.S. site (or at least block all offending items on its U.S. site from being accessible in France)[137] and pay the equivalent of $13,000 per day for every day it did not comply. It also ordered Yahoo France to post warnings on its French language site that accessing sites in other jurisdictions that violate French law on Nazi memorabilia or racism and could lead to criminal prosecution. The French judgment was upheld on appeal[138] and the award eventually grew to

---

[132] "German Multimedia Law": Gesetz zur Regelung der Rahmenbedingungen für Informations und Kommunikationsdienste [IuKDG], § 5 (June 13, 1997). Under the now-repealed law, online providers anywhere could be prosecuted for offering a venue for content illegal in Germany if they do so knowingly and it was "technically possible and reasonable" to prevent it. The law and its worldwide applicability were upheld in 2000 by the German Supreme Court: decision of 12 Dec. 2000, BGH Urteil No. 1 StR 184/000.

[133] Amtsgericht München (local court, Munich), AZ 8340 Ds 465 Js 173158/95 (July 15, 1998).

[134] An English-language report of the matter is available at www.nytimes.com/library/tech/98/05/biztech/articles/29compuserve.html. Years later, the decision was reversed on appeal. See www.nytimes.com/1999/11/18/business/international-business-german-court-overturns-pornography-ruling-against.html.

[135] Wilson, "Net Porn Baron Escapes Jail," The Guardian (London) (Sept. 7, 1999), p. 5, available at www.guardianunlimited.co.uk/Archive/Article/0,4273,3899327,00.html.

[136] Association Union des Etudiants Juifs de France et Ligue Contre le Racisme et l'Antisemitisme v. Yahoo! Inc., Tribunal de Grande Instance de Paris, Ordonnance de Référé, rendue le 22 mai 2000. English translation available at www.lapres.net/yahen.html.

[137] It is interesting that, sixteen years later in the Google Spain case discussed below, Google reluctantly agreed to do almost exactly the same thing: it agreed to remove, from search results available to IP addresses within the European Union, all links to information that was "delisted" under European law.

[138] Association Union des Etudiants Juifs de France v. Yahoo!, Inc., Tribunal de Grande Instance de Paris (Nov. 20, 2000),

more than $5 million. Yahoo filed an action in federal court in California to have the French court's decision declared unenforceable in the U.S., but it was not until an appeal years later[139] that Yahoo was able to have the French judgment overturned, at a substantial cost.

This case was viewed by many international attorneys and scholars as the beginning of a trend toward restrictive nationalism and nation-by-nation censorship, forcing companies to show only particular content to particular countries. The steering committee chairman of the American Bar Association's "Jurisdiction in Cyberspace" program reacted this way: "Are we prepared to let 206 countries regulate the content on the Internet . . . based on the fact that it's there and they can see it?"[140]

[D]—Italian Indictment of Google Executives

In 2006, some Italian teens uploaded to Google Video, a video hosting site, a three-minute clip of themselves bullying a seventeen-year-old boy with Down Syndrome. Google deleted the video after being notified by Italian law enforcement authorities that the clip was illegal under Italian law. Almost two years later, Italian prosecutors decided to indict several Google executives, residents of California who had never set foot in Italy while employed at Google, for failing to monitor the American video site for content that violated Italian law. Prosecutors sought one-year prison terms. One of the defendants stated in his blog at the time:

"Italy has a legal concept which is unknown in Anglo-Saxon countries: namely, that an employee of a company can be held personally criminally liable for the actions or non-actions of the corporation he works for. Moreover, Italy has also criminalized much of its data protection laws, meaning that routine data protection questions can give rise to criminal prosecutions. . . . [I]magine the consequences if every data protection decision made by a company can be second-guessed by a public prosecutor with little knowledge of privacy law. Does that mean that a data protection lawyer working for a company is running the risk of personal criminal arrest and indictment and prosecution for routine business practices? Well, I guess

---

available at http://www.lapres.net/yahen11.html.

[139] Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme, 433 F.3d 1199 (9th Cir. 2006). In 2012, the same group that had demanded the removal of offending content from Yahoo! contacted Twitter and demanded that Twitter remove anti-semitic posts and photos under threat of yet another lawsuit. Twitter complied, not because it was willing to subject its entire website to French law, but because the posts violated Twitter's terms of service—which provided that Twitter would remove posts in countries where they violate the law. Erlanger and Cowell, "Twitter Removes Anti-Semitic Postings, French Jewish Group says," New York Times (Oct. 19, 2012). The lawsuit, however, was not over. A French court ordered Twitter to turn over the identities of the individuals who posted the offending content. Twitter resisted, since its data are stored only in the U.S., but ultimately, after discussions with French authorities, agreed to disclose the information.

[140] Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdictional Issues Created by the Internet, 55 Bus. Law. 1801, 1883 (2000), available at http://works.bepress.com/margaret_stewart/1/. As if to confirm the warning bells set off by the Yahoo France case, Canada has joined the fray. A Canadian company, Equustek Solutions, Inc., obtained a court order requiring Google to de-list from its search results all references to another company that had been found to have violated Canadian law—not only from Google's Canadian website, but worldwide. Google appealed all the way to the Canadian Supreme Court but was unsuccessful, and notwithstanding a subsequent U.S. federal court order barring enforcement of the decision, the Canadian courts refused to modify the order. The Equustek case is further discussed below.

you can see why I've been advised not to set foot in Italy."[141] Three of the executives, including Google's Global Privacy Counsel, were convicted in absentia for criminal violations of Italy's privacy laws.[142]

[E]—Brazilian Indictment of Google Executive

In 2012 a Google executive in Brazil, a Brazilian citizen, was arrested (and apparently only briefly detained) when Google refused to take down videos criticizing a local mayoral candidate.[143] Notwithstanding these few cases, claims by one nation that its online laws applied extraterritorially were rare.[144] Instead, national governments limited their international efforts to blocking content, cooperating with international criminal law enforcement efforts, and requesting that foreign online providers voluntarily remove or block in-country access to content that violates that country's domestic laws—requests that online providers were often willing to grant.[145]

[ii]—Challenges to Traditional Limits

[A]—The Snowden Effect

The revelations, beginning in May 2013, that the United States was engaging in a massive electronic spying program that, among other things, targeted the entire population of the European Union, sent shockwaves across the continent. Reactions were immediate and profound. In June, the *New York Times* ran an article by a German politician pointing out, by way of comparison, that a German

---

[141] "Ciao, Italia!," Fleischer blog (Nov. 24, 2009), available at http://peterfleischer.blogspot.com/2009/11/ciao-italia.html.

[142] The background of this case is discussed in Donadio, "Larger Threat is Seen in Google Case," New York Times (Feb. 24, 2010), available at http://www.nytimes.com/2010/02/25/technology/companies/25google.html?partner=rssnyt&emc=rss.

[143] Reported by numerous sources, e.g., Brocchetto, "Brazilian Police Arrest Google Exec Over Online Videos," CNN, (Sept. 26, 2012), available at http://www.cnn.com/2012/09/26/tech/brazil-google/.

[144] France, however, never changed its position. In 2015, the French government issued Decree 2015-253, requiring every search engine in the world to delist websites related to terrorism or child pornography. Décret n° 2015-253 du 4 mars 2015 relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique. Also in 2015, a French court claimed that it had jurisdiction over a case in which a resident of Paris was suing Facebook, a California company—not for refusing to block content as in the Yahoo case discussed above, but for blocking content. The plaintiff had posted an image of a 19th century photorealistic painting that depicted a reclining woman with her vagina exposed, and in response Facebook blocked his account for violating its terms of service. Plaintiff's counsel claimed that the provision in Facebook's terms of service requiring that all litigation must be conducted in California under California law was just "an attempt to evade French law," and the court found that provision to be "abusive." After a French appellate court ruled that French courts had jurisdiction, the plaintiff's suit against Facebook was allowed to proceed. Reported by numerous news sources, e.g., Larson, "French court rules man can sue Facebook over century-old painting," The Daily Dot (Feb. 14, 2016), available at http://www.dailydot.com/technology/vagina-painting-france-sue-facebook/. After several years of litigation, the case was settled in August 2019.

[145] In 2012, Twitter granted a German government request that it block users in Germany from accessing a neo-Nazi account. "Twitter neither shut down the group's account nor deleted the group's posts. It blocked them for users only in Germany, who see a message that reads 'Blocked' and 'This account has been withheld in Germany,' along with a link to more information about the policy." Kulish, "Twitter Blocks Germans' Access to Neo-Nazi Group," New York Times (Oct. 18, 2012). In Equustek Solutions Inc. v. Google, Inc., 2-15 BCCA 265 (Court of Appeal for British Columbia June 11, 2015), discussed below, in response to demands that it remove links to sites found damaging to a Canadian company, Google was willing to remove search listings from google.ca but not worldwide.

law that had merely mandated the retention of communications metadata (no content) for law enforcement purposes had been ruled unconstitutional:

"Germans have experienced firsthand what happens when the government knows too much about someone. . . . [W]e have not forgotten what happens when secret police or intelligence agencies disregard privacy. It is an integral part of our history and gives young and old alike a critical perspective on state surveillance systems. . . . When courts and judges negotiate secretly, when direct data transfers occur without limits, when huge data storage rather than targeted pursuit of individuals becomes the norm, all sense of proportionality and accountability is lost."[146]

An official letter from the European Commission to the United States demanded immediate answers to a series of interrogatory-style questions regarding U.S. surveillance.[147] The Commission set up a Working Group to determine what actions to take regarding numerous U.S.-European data exchange programs.[148] The Commission also issued a position paper[149] calling for a top-to-bottom reassessment of data exchange programs with the U.S., stating: "Massive spying on our citizens, companies, and leaders is unacceptable. . . . European citizens' trust has been shaken by the Snowden case, and serious concerns still remain. . . ."[150] Many commentaries claimed that the American surveillance program violated international legal norms such as the European Convention on Human Rights, and extraterritorial application of fundamental European rights became a hot topic of discussion among European legal experts.[151] Relationships between the United States and Europe underwent a sea change regarding all manner of data transfers.[152]

In the wake of the Snowden revelations, the European Union has taken a determined, even aggressive, approach to extraterritorial application of its online laws and privacy protections. In an online context, the traditional limits on extraterritorial application of foreign, in particular European, substantive law to persons within the United States are being challenged.

---

[146] Spitz, "Germans Loved Obama. Now We Don't Trust Him," New York Times (June 29, 2013).

[147] "[The EU has] serious concerns about recent media reports that United States authorities are accessing and processing, on a large scale, the data of European Union citizens using major US online service providers." Letter from Viviane Reding, Vice President of the European Commission, to Attorney General Eric Holder, June 10, 2013, p.1.

[148] The programs targeted for Commission scrutiny included the now-defunct Safe Harbor, which exempted American companies from most of the strict requirements of the European Privacy Directive, the airline Passenger Name Record agreement (CE Memo 13/1054), and the Terrorist Finance Tracking Programme (CE Memo 13/1060).

[149] European Commission, "Rebuilding Trust in EU-US Data Flows," Communication from the Commission to the European Parliament and the Council, COM(2013) 846, Nov. 26, 2013.

[150] European Commission, "European Commission calls on the U.S to restore trust in EU-U.S. data flows," Press Release, Nov. 27, 2013.

[151] See, e.g., Kuner, "Extraterritoriality and the Fundamental Right to Data Protection," Blog of the European Journal of International Law, Dec. 16, 2013.

[152] "Germany has curbed its cooperation with United States intelligence, pushing back against a key ally amid new revelations of spying on Germans and other Europeans that have set off a domestic firestorm." Smale, "Germany Limits Cooperation with U.S. Over Data Gathering," New York Times (May 7 2015), available at http://nyti.ms/1FRM29t.

[B]—The Demise of the EU Privacy Directive and the Replacement of Its 'Safe Harbor' with the Privacy Shield

For more than thirty-five years, the 1995 European Union Data Protection Directive,[153] also called the "Privacy Directive,"[154] and its 1981 predecessor, the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,"[155] were not viewed as presenting any problems of extraterritoriality. The 1981 Convention introduced the concepts, now common in Europe and elsewhere, of "data protection," "data subject," and "data controller," and contained provisions such as limits on the collection of personal data, the right of individuals to access and correct information about themselves, and the right to pursue legal remedies if they are unable to do so.[156]

The Privacy Directive provided that transferring personal data regarding EU residents from anywhere within the EU to anywhere outside the EU was prohibited unless the country to which the data are being transferred has implemented legally binding data protection standards that provide an adequate level of protection for such data.[157] It gradually became the *de facto* world standard (at least outside of the United States) for online privacy practices. Many countries have used it as a model for their own legislation. The privacy standards adopted[158] by the member nations of the Asia-Pacific Economic Cooperation controller (APEC)[159] are based in part on the Privacy Directive. Uruguay enacted a data protection law explicitly modeled on the Privacy Directive, to attract outsourcing.[160]

For decades, European nations did not attempt to apply the Privacy Directive extraterritorially; rather, they focused on enforcing it regarding data within the EU, including data sent from the EU to companies outside the EU. Europe was trusting and accommodating. The EU even worked out a set of "Safe Harbor" principles

---

[153] Directive 95/46/EC (24 Oct. 1995): On the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. L 281, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf. The Privacy Directive is supplemented by Regulation (EC) No 45/2001 (18 Dec. 2000), "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," available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/Legislation/Reg_45-2001_EN.pdf regarding the European Community organizations themselves, and by Directive 2002/58/EC (the "ePrivacyDirective," available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML.

[154] "The current data protection framework in the EU is 20 years old this year. That's 20 years ago . . . when the internet was in its infancy [and] when mobile phones penetrated only about 10% of the population [of] the US and Western Europe." Butarelli, European Data Protection Supervisor, Speech before Council on Foreign Relations, Washington D.C. (March 10, 2015).

[155] Council of Europe, European Treaty Series No. 108 (Strasbourg, Jan. 28, 1981).

[156] Convention, Arts. 5 and 8.

[157] Privacy Directive, N. 100 *supra*, Art. IV, § 25. The Privacy Directive is not directly applicable as law itself, but rather, each European Union member state must enact legislation implementing the Directive. All member states have done so.

[158] APEC Cross-Border Privacy Rules System (2005), Policies, Rules and Guidelines, http://www.cbprs.org/.

[159] Australia, Brunei, Canada, Chile, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Taiwan, Thailand, and Viet Nam. The U.S. is also a member.

[160] Personal Data Protection Law 18331, 208 PRA (Oct. 29, 2007).

allowing U.S. companies to self-certify that they were meeting the standards set forth in the Privacy Directive for data transferred from Europe.[161]

The Snowden revelations changed all that. A series of inquiries, official statements, court decisions, and legislative initiatives made it clear that when it came to international data transfers, the trusting relationship between the U.S. and the EU was no more; mistrust and to some extent outright hostility became the norm. The Safe Harbor arrangement was itself a casualty of the Snowden revelations, as set forth in an official statement of the European Commission: "[The] fundamental basis of the Safe Harbour has to be reviewed in the new context of . . . the information recently released on US surveillance programmes which raises new questions on the level of the protection the Safe Harbour arrangement is deemed to guarantee."[162] The Advocate General of the Court of Justice of the European Union also came out with an official opinion that the Safe Harbor should be invalidated, stating that "in the light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency 'the NSA'), the law and practices of the United States offer no real protection against surveillance by the United States of the data transferred to that country."[163] Shortly thereafter, the Court of Justice of the European Union held that the Safe Harbor was invalid, effective immediately.[164] Since the Safe Harbor arrangement was merely an agreement between the U.S. and the EU, the court's decision terminating it, while expressing extreme displeasure at the U.S., did not constitute an attempt to apply European law extraterritorially. Nonetheless, suddenly hundreds of European companies found themselves transferring data to U.S. companies without any legal basis for doing so.

Rather than consider cutting off data transfers, the European Commission and the U.S. Department of Commerce quickly worked out an alternative arrangement, called the Privacy Shield, which took effect on August 1, 2016.[165]

[C]—Google Spain: The Right-to-Be-Forgotten Decision

The first major court ruling that reflected the post-Snowden mistrust by actually applying European law extraterritorially was the 2014 European Court of Justice decision known as *Google Spain* or "Right To Be Forgotten" (RTBF) case.[166] That

---

[161] European Commission, Decision 2000/520 (July 26, 2000).

[162] European Commission, "Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU," COM 847 (Nov. 27, 2013), p. 2.

[163] Advocate General's Opinion in Case C-362/14, Court of Justice of the European Union Press Release No. 106/15 (Sept. 23, 2015), p. 1.

[164] Schrems v. Data Protection Commissioner, CJEU Case C-362/14 (Oct. 6, 2015). Although the *Schrems* case was widely reported, its the EU did not suddenly start initiating enforcement actions; instead the EU and U.S. came up with the Privacy Shield.

[165] The full text of the Privacy Shield, along with letters of transmittal and a statement of principles, may be found on the Department of Commerce website at https://www.privacyshield.gov/eu-us-framework.

[166] Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12 (ECJ May 13, 2014) (not to be confused with the "right to be forgotten" provision in the EU's General Data Protection Regulation (GDPR), discussed below).

decision held, for the first time, that the Privacy Directive applies extraterritorially, and that Google (and by implication every search engine company in the world) must, at the request of any EU citizen, remove from search results all data about that citizen, effectively allowing each EU citizen to control search engine results pertaining to himself or herself. The court's opinion, which was overturned in practice but not in principle in 2019 by Europe's highest court, in an opinion[167] that confirmed European Union's power to apply the RTBF worldwide but interpreting the law as simply not (yet) having done so, is remarkable for a number of reasons.

First, the RTBF as so interpreted challenges a basic premise of the Internet: that search engines may freely index online information. The court's mandate as well as the 2019 opinion are directed only at search engines; the websites actually containing the delisted material are unaffected.[168] Moreover, the mandate is not limited to material that is illegal or defamatory; URLs containing material that is legally posted and non-defamatory must be delisted on demand as well. Google and a number of *amici* had argued that since search engines merely index what is already posted online, "any request seeking the removal of information must be addressed to the publisher of the website concerned because it is [the publisher] who takes the responsibility for making the information public," and that a government authority should be able to order a search engine "to erase information published by third parties from its filing systems only if the data in question have been found previously to be unlawful or incorrect. . . ."[169] The court rejected these arguments, specifically holding that "the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information related to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful."[170] The court further stated that for a search engine to be required to suppress information, "it is not necessary . . . that the inclusion of the information in question in the list of results causes prejudice to the [citizen]."[171]

---

[167] Google LLC v. Commission nationale de l'informatique et des libertés, Case C-507/17 (CJEU Sept. 24, 2019),

[168] *Id.*, ¶ 84. "Given the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, effective and complete protection of data users could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the publishers of websites." This passage is perhaps one of the most revealing of the court's post-Snowden mistrust of all things American: The court had no problem applying the Privacy Directive extraterritorially to a U.S. search engine but refrained from applying the same standard to websites in Europe and elsewhere containing the actual information in question. Another example: Paragraph 72 treats indexing of web content that is presumed to be lawful as the type of processing that must be done "fairly" and "Lawfully" and "collected for specified, explicit, and legitimate purposes" and that the data collected must be "adequate, relevant, and not excessive in relation to the purposes for which they are collected," but ignores the data collected on the original website in question. Similar passages can be found throughout the opinion.

[169] *Id.*, ¶¶ 63-64.

[170] *Id.*, ¶ 88. (Emphasis supplied.)

[171] *Id.*, ¶ 96.

Second, the RTBF also challenges the notion of free expression, a free press, and the free flow of information. By allowing anyone to censor search results about himself or herself, the decision drastically decreases the utility of search engines, since anyone in the European Union can suppress anything about themselves, not only articles or blog posts they may have written, but also significant information such as reports of criminal convictions or shady business practices. In just the first three days after the court decision was made public, those who demanded that their names be de-listed included "20 convicted criminals, . . . a paedophile, . . . a man convicted of possessing child abuse images, and a [physician] who received negative reviews from patients. . . ."[172] Many journals decried the fact that pursuant to *Google Spain*, the UK Information Commissioner even ordered Google to remove links to news stories about the fact that the Information Commissioner had ordered Google to remove links to news stories.[173]

Third, *Google Spain* takes the concept of outbound application of substantive law to a whole new level: according to the ECJ, its decision applies worldwide.[174] The 2019 decision limiting the *Google Spain* to search engine results within the EU was an interpretation of applicable legal provisions, but not the right of the EU to enact legislation applicable worldwide.[175]

Criticism of the 2014 RTBF decision was immediate and widespread. The *New York Times* editorialized that the decision "sets a terrible example for officials in other countries who might also want to demand that Internet companies remove links they don't like."[176] Other commentators decried the ruling as senseless: "The ruling appears to mean that if a French person requests that Google take down links to

---

[172] Warman, "Ex-MP asks Google for 'right to be forgotten,'" Daily Telegraph (UK) (May 16, 2014), available at http://www.telegraph.co.uk/technology/google/10834651/Ex-MP-asks-Google-for-right-to-be-forgotten.html.

[173] Information Commissioner's Office, "Data Protection Act 1998, Supervisory Powers of the Information Commissioner, Enforcement Notice," Aug. 18, 2015/Aug. 20, 2015, available at https://ico.org.uk/action-weve-taken/enforcement/google-inc/. For a typical news report about the notice, see Gibbs, "Google ordered to remove links to 'right to be forgotten' removal stories," The Guardian (UK) (Aug. 20, 2015), available at http://www.theguardian.com/technology/2015/aug/20/google-ordered-to-remove-links-to-stories-about-right-to-be-forgotten-removals.

[174] The fact that a search engine was indexing online information regarding European citizens, was not, by itself, the basis upon which the ECJ decided that the RTBF ruling should be enforced against Google: "Google Search does not merely give access to content hosted on the indexed websites, but takes advantage of that activity and includes, in return for payment, advertising associated with the internet users' search terms, for undertakings which wish to use that tool in order to offer their goods or services to the internet users." *Id.*, ¶ 43. Thus, for at least jurisdictional purposes, the ECJ was basing its "minimum contacts" analysis on advertising directed at Spain. "Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State." *Id.* Nonetheless, the court largely ignored this jurisdictional analysis when issuing its sweeping mandate regarding search engines throughout the world.

[175] "While the EU legislature has . . . struck a balance between that right [to be forgotten] and that freedom [of information online] so far as the [European] Union is concerned . . . , it must be found that, by contrast, it has not, to date, struck such a balance as regards the scope of a de-referencing outside of the Union. . . . It follows that *currently*, there is no obligation under EU law, for a search engine operator who grants a request for de-referencing made by a data subject . . . to carry out such a de-referencing on all the versions of its search engine." Google LLC v. Commission nationale de l'informatique et des libertés, Case C-507/17 (CJEU Sept. 24, 2019), pars. 60 and 64 (emphasis added).

[176] Editorial, "Europe's Expanding 'Right to Be Forgotten,'" New York Times (Feb. 4, 2015), available at http://www.nytimes.com/2015/02/04/opinion/europes-expanding-right-to-be-forgotten.html.

some old, negative (but truthful) information about them, then Google must remove links to that info globally, even in countries outside Europe. It is as bizarre as it sounds: The ruling . . . insists that a few judges in France, and Europe more broadly, get the final say on what Google can and cannot link to in search results. Those judges claim the right to censor web search results globally."[177] Google itself posted a detailed criticism of the decision on its official blog, stating:

> "While the right to be forgotten may now be the law in Europe, it is not the law globally. Moreover, there are innumerable examples around the world where content that is declared illegal under the laws of one country, would be deemed legal in others: Thailand criminalizes some speech that is critical of its King, Turkey criminalizes some speech that is critical of Ataturk, and Russia outlaws some speech that is deemed to be 'gay propaganda.' If the CNIL's proposed approach were to be embraced as the standard for Internet regulation, we would find ourselves in a race to the bottom. In the end, the Internet would only be as free as the world's least free place."[178]

Google decided to resist. In response to the decision, the company created a legalistic opt-out form[179] for people to fill out and submit. The form required that people wanting to be removed from search results submit copies of identification documents. For forms that Google deemed acceptable, Google would remove search results only for EU domains, but not any other domains such as .com or .net.[180] The data protection authorities in the EU were not pleased. The Article 29 Data Protection Working Party, an official group comprising the European Commission, the EU Data Protection Supervisor, and the privacy commissioners from each EU member state's Data Protection Authority, took the unusual step of issuing guidelines[181] specifically addressing the Right-To-Be-Forgotten case and how it must be implemented. The Working Party confirmed that from an EU perspective the RTBF decision had worldwide extraterritorial effect: "In order to give full effect to the data subject's rights as defined in the Court's ruling, de-listing decisions must be implemented in such a way that they guarantee the effective and complete

---

[177] Edwards, "France just made a serious (and scary) bid to put itself in charge of internet censorship, globally," Business Insider (Sept. 22, 2015), available at http://www.businessinsider.com/france-cnil-ruling-google-right-to-be-forgotten-globally-2015-9?r=UK&IR=T.

[178] Google, "Implementing a European, not global, right to be forgotten," Google Europe Blog (July 30, 2015), http://googlepolicyeurope.blogspot.com/2015/07/implementing-european-not-global-right.html.

[179] "Search removal request under data protection law in Europe," https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=en (still online in November 2019). The form demands copies of identity documents and specific "URLs for results you want removed."

[180] Prior to the decision, when a French lawyer demanded that Google remove its links to purportedly defamatory material, Google did so, but only on its French site. The lawyer sued Google in France, demanding that Google remove all search links, not just the French ones, and won. In French: M. et Mme X et M. Y / Google France, Tribunal de grand instance de Paris, Ordonnance de r éféré du 16 septembre 2014, available at http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4291. Google then removed all the search links for its European domains, but not the .com ones, taking the position that no European court had jurisdiction over non-European domains.

[181] Article 29 Data Protection Working Party, "Guidelines on the Implementation of the Court of Justice of the Euopean Union Judgment on 'Google Spain [SL] and [Google] Inc. v. Agenciea Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/12" (Nov. 26, 2014) (English version is 14/EN WP 225).

protection of data subjects' rights and that EU law cannot be circumvented. In that sense, limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the ruling. In practice, this means that in any case de-listing should also be effective on all relevant domains, including.com."[182] The Working Party went even further: The guidelines state: "Search engine managers should not as a general practice inform the webmasters of the pages affected by de-listing of the fact that some webpages cannot be acceded from the search engine in response to specific queries."[183] Nonetheless, Google ultimately prevailed, at least with regard to that specific case, in the 2019 CJEU decision discussed above.

[D]—The Google France RTBF Decision

A few months later, a French court issued a similar ruling regarding a lawyer who had demanded that Google delist all search results linking to purportedly defamatory material about him. Google did so, but only on its French site. The lawyer sued Google France, demanding that Google remove all search links, not just the French ones, and won.[184] Google responded by delisting the search results for European domains, but refused to delist search results on the .com domain, claiming that the French court had no jurisdiction over .com domains or Google France's U.S. parent.[185] The French Data protection authority CNIL issued a formal notice to Google, ordering it to delist RTBF content on all domains, not just European ones,[186] and threating Google with huge fines (up to $2.5 billion) if it did not comply.[187] Like its counterpart in Spain, the French court had no problem with the fact that original source materials would not be affected; in fact, CNIL pointed out that the decision "does not require deletion of the link from the indexes of the search engine altogether. That is, the original information will still be accessible using other search terms, or by direct access to the publisher's original source."[188] The 2019 *Google v. Commission* decision discussed above effectively overturned the *Google France* decision.

[E]—Google Canada: The Equustek Decision and the "Extraterritorial Effect" Doctrine

---

[182] *Id.*, ¶ 7.

[183] *Id.*, ¶ 9. The 'gag order' prohibiting notification of websites that they are being de-listed seems uncomfortably similar to the 'gag orders' contained in "national security letters" issued in the United States under the Patriot Act.

[184] M. et Mme X et M. Y / Google France, Tribunal de grand instance de Paris, Ordonnance de r éféré du 16 septembre 2014, available at http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4291.

[185] Scott, "A Question Over the Reach of Europe's 'Right to Be Forgotten,'" New York Times (Feb. 2, 2015), available at http://bits.blogs.nytimes.com/2015/02/01/questions-for-europes-right-to-be-forgotten/?_r=0.

[186] "CNIL orders Google to apply delisting on all domain names of the search engine," CNIL News (June 12, 2015), available at https://www.cnil.fr/fr/node/15790.

[187] An English-language report can be found at Moody, "France tells Google to remove search results globally, or face big fines," Ars Technica (Sept. 21, 2015), available at http://arstechnica.com/tech-policy/2015/09/france-confirms-that-google-must-remove-search-results-globally-or-face-big-fines/.

[188] "CNIL orders Google to apply delisting on all domain names of the search engine," N. 142 *supra*.

Later that same year, in a Canadian case[189] often referred to as "*Google Canada*," a British Columbia court ordered Google to delist certain Canadian websites from search results.[190] Approaching the matter as it did in *Google Spain*, Google offered to delist results for Canadian domains, but not on its main .com site, arguing that the court had no jurisdiction over Google in California, and that even if it did, the court had no authority to issue a worldwide order.

The court's analysis of online extraterritoriality in *Google Canada* is worthy of attention for several reasons. First, the court's opinion, while citing *Google Spain*, is significantly more thoughtful and analytical than its European counterpart—completely devoid of the post-Snowden hostility that subtly permeates the *Google Spain* opinion. More significantly, the *Google Canada* court came up with a much stronger rationale for ordering worldwide delisting.

As a preliminary matter, the court stated that traditional common-law limitations on jurisdiction no longer apply: "The Supreme Court of Canada has recognized that the law has evolved to allow courts to deal with disputes arising in an increasingly interdependent global economy. In its recent jurisprudence, the Supreme Court has reasoned that, in the proper case, the limits of the courts' jurisdiction should be expanded, not narrowed."[191] The result: "There now seems little doubt that Canadian courts actually have the power to employ *in personam* orders to enjoin parties to do or refrain from doing something anywhere in the world."[192] Citing *Google Spain* as precedent, the Canadian court held that because Google Inc. in California sold search engine advertising directly to Canadian residents, it was doing business in Canada and was thus subject to the court's jurisdiction.[193]

The court rejected Google's argument that if a Canadian court could order a California corporation to remove content, every country in the world could do the same, creating chaos for Google: "That may be so. But if so, it flows as a natural consequence of Google doing business on a global scale, not from a flaw in the territorial competence analysis."[194] Moreover, the court rejected the very notion that it was applying national law extraterritorially: "Further, the territorial competence analysis would not give every state unlimited jurisdiction over Google; *jurisdiction will be confined to issues closely associated with the forum. . . .*"[195] In other words, requiring a foreign online company to suppress content related to the forum was not an extraterritorial application of substantive law at all; the order

---

[189] Equustek Solutions Inc. v. Jack, 2014 BCSC 106 (June 13, 2014).

[190] Unlike the situation in *Google Spain*, Google was not named as a party but was merely enjoined by a court order. Also, in contrast to *Google Spain*, which involved the delisting of websites that were legal, the Canadian websites ordered to be delisted were illegal in Canada. The defendants had ignored numerous injunctions and continued to "carry on business [selling counterfeit goods] through a complex and ever expanding network of websites." *Id.*, ¶ 7.

[191] *Id.*, ¶ 103, (quoting Mineral Aquiline Argentina SA v. IMA exploration Inc., 2007 BCCA 319, ¶ 92).

[192] *Id.* ¶ 126 (quoting Black and Babin, "Mareva Injunctions in Canada: Territorial Aspects,"28 Can Bus L.J. 430, 441 (1997).

[193] *Id.*, ¶¶ 57-60.

[194] *Id.*, ¶ 64.

[195] *Id.* (Emphasis added.)

merely had *extraterritorial effect*. This approach was greeted with enthusiasm within the European Union.[196] The Supreme Court of Canada dismissed the appeal, issuing a short opinion that added no further analysis, but that did leave the door slightly open to Google: "If Google has evidence that complying with such an injunction would require it to violate the laws of another jurisdiction, including interfering with freedom of expression, it is always free to apply to the British Columbia courts to vary the interlocutory order accordingly."[197] Google then filed a declaratory judgment action in a California federal court, asking the court to enjoin enforcement of the Canadian order in the United States (and apparently anywhere outside Canada). Equustek refused to participate in the federal court proceedings. Google won a default judgment and a permanent injunction barring enforcement of the order based on the court's finding that the Canadian order deprived Google of the protections of U.S. federal law, namely the immunity provided in Section 230 of the Communications Decency Act.[198] With the ink on the declaratory judgment barely dry, Google then took the Canadian Supreme Court up on its offer, and applied to the Supreme Court of British Columbia to modify or lift its worldwide injunction. In 2018 that court dismissed the application,[199] leaving the Canadian injunction in place, and leaving Google with two diametrically opposed court orders.

The "Extraterritorial Effect" doctrine set forth in *Google Canada* is part of a major transformation of international Internet law: it not only reinforces the European view that a court in one country can order worldwide suppression of online content but also marks the beginning of a shift of the burden of content suppression: Prior to these delisting cases, governments that wanted to censor the Internet took it upon themselves to do so using technical measures; sometimes they implemented nationwide blocking of content located at foreign IP addresses or forced foreign online companies to install censorship firewalls (as in the case of China), but even countries with strict censorship regimes refrained from attempting to impose extraterritorial suppression of content.

The Extraterritorial Effect doctrine has created a content suppression model that closely resembles the early failed attempts by courts in France and Germany to apply national law extraterritorially to American online companies. In those early cases, the plaintiffs had likewise demanded that content that was illegal under their national laws be suppressed *within their own countries.*[200] Those early cases,

---

[196] "While Articles 25 and 26 [of the EU Data Protection Directive] may not explicitly refer to conduct occurring outside the EU, and thus may not be regarded as extraterritorial in scope within a literal meaning of the term, they do have extraterritorial effect." Kuner, "Extraterritoriality and International Data Transfers in EU Data Protection Law," U. Cambridge Legal Studies Research Paper No. 49/2015 (Aug. 2015), p. 2.

[197] Google Inc. v. Equustek Solutions Inc., Supreme Court of Canada, Case No. 36602 (June 28, 2017). 2017 SCC 34, ¶ 36.

[198] Google LLC v. Equustek Solutions Inc., No. 5:17-CV-04207-EJD (Order Granting Plaintiff's Motion for Default Judgment and Permanent Injunctive Relief), (N.D. Cal. Dec. 14, 2017).

[199] Equustek Solutions Inc. v. Jack, 2018 BCSC 610 (April 16, 2018). The British Columbia Supreme Court, obviously annoyed that its order was being challenged, disagreed with, and mischaracterized, the U.S. federal court's analysis of U.S. law: "The U.S. decision does not establish that the [Canadian] injunction requires Google to violate American law. . . . Google has not demonstrated that the injunction violates core American values."

[200] *Google France* did not involve an attempt to force worldwide removal of the Nazi paraphernalia at issue; the plaintiffs and

however, involved attempts to force U.S. online companies to suppress content that was not only legal in the U.S., but that had nothing whatever to do with France or Germany. The Extraterritorial Effect doctrine, by contrast, holds that a court in Country A can order a company located in Country B to suppress online content to the extent that the content (1) is about individuals in Country A, and (2) is accessible in Country A. The doctrine thus not only requires that the content in question pertain to the forum, but also calls for "location based, rather than domain-based, delisting."[201] The advantage of this approach is that "location-based delisting seems to be a more credible basis for search engines to give full effect to European law, within the framework of their responsibilities, powers, and capabilities, while also avoiding some of the perceived challenges of global delisting."[202]

[F]—The Belgian Facebook Case

Although *Google Spain* and *Google Canada* set the new paradigms, a number of other cases decided by foreign courts followed in their footsteps.[203] In one such case a court in Belgium, in effect applying the Extraterritorial Effects doctrine, ordered Facebook, Inc. and its European affiliates to cease registering (via cookies and plug-ins) the websites Belgian Internet users who do not have Facebook accounts visit.[204]

[G] – The Austrian Facebook Case:

In 2019 the Europe's highest court, the Court of Justice of the European Union (CJEU), went far beyond the *CompuServe* and *Yahoo France* cases discussed above, and ruled that the eCommerce Directive of 2000[205] empowers any local court in any EU member state to enjoin online hosting providers, no matter where located, to block access, *anywhere in the world,* to material the local court finds to be defamatory, infringing, or otherwise illegal.[206] The CJEU opinion is surprisingly simplistic, merely giving lip service to international law: "It is apparent from [the eCommerce Directive] that, in view of the global dimension of electronic commerce,

---

the court both made it clear that they demanded only that the material not be accessible in France, from any website.

[201] Powles, "The Contested Map of the 'Right to Be Forgotten,'" Slate (Feb. 15, 2015), available at http://www.slate.com/articles/technology/future_tense/2015/02/google_and_the_right_to_be_forgotten_should_delisting_be_global_or_local.html.

[202] *Id.* (quoting from *Google Spain*).

[203] "It is a challenge being faced on a global scale, from Canada to Australia, and Japan to Spain." O'Doherty, "Data hosts and obligations under data protection legislation," 23 The Bar Review (Ireland) No. 2 (April 2018), p. 44 (citing examples).

[204] Court of First Instance Brussels, No. 15/57/C, 9 Nov. 2015 (in Dutch), available at https://www.privacycommission.be/sites/privacycommission/files/documents/Vonnis%20Privacycommissie%20v.%20Facebook%20-%2009-11-2015.pdf. The court imposed a fine of 250,000 Euros per day of noncompliance. Facebook complied but appealed, and in June 2016 the Brussels Court of Appeals vacated the decision; further proceedings were pending as of late 2016. Belgium Privacy Commission, "La Cour d'appel rejette les arguments contre Facebook" (Press release in French), (June 30, 2016), available at https://www.privacycommission.be/fr/news/la-cour-dappel-rejette-les-arguments-contre-facebook.

[205] Directive 2000/31/EC (June 8, 2000).

[206] Glawischnig-Piesczek v. Facebook Ireland Ltd., CJEU No. C-18/18, par. 53 (Oct. 3, 2019): "Directive 2000/31, in particular Article 15(1), must be interpreted as meaning that it does not preclude a court of a Member State from . . . ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law."

the EU legislature considered it necessary to ensure that EU rules in that area are consistent with the rules applicable at international level. It is up to Member States to ensure that the measures which they adopt and which produce effects worldwide take due account of those rules."[207] Having emanated from the CJEU, the case cannot be appealed. Nonetheless, the decision has faced widespread criticism, and its vague language raises more questions than it answers.

[H]—The General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR),[208] proposed in 2012 as a replacement for the Privacy Directive, became law on May 24, 2016; enforcement began two years later, starting on May 25, 2018.[209] The GDPR is a set of rules restricting how companies anywhere in the world may collect and process data regarding persons living in the European Union. The GDPR grants specific privacy rights to all Europeans and contains detailed requirements all companies in the world must adhere to, to ensure that these privacy rights are respected. The GDPR has global significance because it applies to any company in the world that collects, processes, disseminates, or stores data about people living in the EU—whether or not the company is physically present there.[210] It has changed the way that companies around the world, including those in the United States, process data pertaining to individuals. It has established a *de facto* world standard for individual data privacy. The EU is serious about implementing the GDPR. The penalties for noncompliance can be huge: up to 20 million Euro, or 4% of a company's global annual revenue, whichever is greater.[211] Because the GDPR targets only privacy

---

[207] Id., Pars. 51-52.

[208] Regulation (EU) 2016/679, 27 April 2016 (General Data Protection Directive (GDPR) "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [Privacy Directive]"). The GDPR applies to the European Economic Area (EEA), meaning all EU countries plus Iceland, Liechtenstein and Norway; nonetheless, since the GDPR itself refers to the EU or Union rather than the EEA, the discussion here will do the same. A separate Privacy Directive was enacted regarding the transfer and processing of investigatory and law enforcement information about individuals: Directive (EU) 2016/680 (April 27, 2016). The EU convention for citing Articles and Paragraphs of the GDPR is not "Art. x Par. y" but "Article x(y)." The GDPR contains roughly 54,000 words. For the full text of the GDPR and related documents, see European Commission, "Reform of EU data protection rules" (Aug. 8, 2016), available at http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

[209] See: European Commission, "Joint Statement on the final adoption of the new EU rules for personal data protection," available at http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm; European Commission, "Reform of EU data protection rules" (Feb. 8, 2016), http://ec.europa.eu/justice/data-protection/reform/index_en.htm. Although the GDPR was proposed prior to the Snowden revelations about just how comprehensive American data collection practices were, those revelations essentially guaranteed rapid promulgation of the GDPR. See discussion at § 11.03[3][b][ii][A] *supra*.

[210] Article 3(2), "Territorial scope," states: "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union." Note that notwithstanding Brexit, the UK has indicated that it will implement a UK version of the GDPR that mirrors the EU version. See Turner, "U.K. to Plan 'Unprecedented Alignment' with EU Over Data Sharing," Bloomberg News (Aug. 23, 2017), https://www.bloomberg.com/news/articles/2017-08-23/u-k-to-plan-unprecedented-alignment-with-eu-over-data-sharing.

[211] Article 83(5) provides that administrative fines up to 20 million Euro or 4% of a company's "total worldwide annual turnover" may be imposed for violations of:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
(b) the data subjects' rights pursuant to Articles 12 to 22;

rights violations that occur in the EU, it is not extraterritorial, and the penalties are thus enforceable against U.S. companies that violate it.[212] The following section in brown-colored font covers the GDPR in much more detail:

The GDPR

The GDPR implements a comprehensive set of rights regarding an individual's personal data, together with a comprehensive regime of data protection obligations applicable to companies that gather and use such data. The individual rights can be summarized[213] as follows:

Informational rights. Individuals have the right to know exactly what information about them is held, how their information is processed, for what purposes, and precisely what organizations have what information.
Right to data portability. Individuals may transfer their data away from one organization and to another.
Right of correction. Individuals may access and correct information that is being stored about them.
Right to be forgotten. Individuals may demand that information about them be deleted when the legitimate purposes for which the data were retained no longer apply.
Right to be informed of data breaches.

The obligations of companies that collect, process, store, or disseminate personal data regarding individuals in the EU can be summarized as follows:

Data collection only with express consent. The company may collect personal data only with the individual's express, opt-in consent.
Full disclosure, obligation to act. The company must inform each person whose data it collects about that person's rights described above, and must act consistently with those rights.

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1)." Article 83(6) provides that fines in the same amount may be imposed for non-compliance with "an order by the supervisory authority as referred to in Article 58(2).

[212] GDPR Art. 3(2). The penalty imposed in the EU would be reduced to a judgment, which would be enforceable in the U.S. pursuant to state law, often pursuant to the Uniform Foreign-Country Money Judgments Recognition Act (which has been enacted by about half the states), or under general common law principles of comity. To enforce a foreign judgment in this country, the European DPA that won the judgment would initiate a civil action in state or federal court to obtain recognition of the foreign-country judgment under the applicable state law. Such recognition could be denied if the court finds that the judgment "is repugnant to the public policy of the State." Uniform Foreign-Country Money-Judgments Recognition Act § 4(b)(3). In this context see Hilton v. Guyot, 159 U.S. 113, 16 S.Ct. 139, 40 L.Ed. 95 (1895). The *Guyot* decision is the basis of American judgment-recognition law to this day; it sets forth common law comity principles. Recognition domesticates the foreign judgment. NOTE, HOWEVER, that U.S. companies that participate in the Privacy Shield program are not subject to such penalties; see the discussion of the Privacy Shield below.

[213] Individual rights summary adapted from European Commission, "Agreement on Commission's EU data protection reform will boost Digital Single Market," Press Release (Dec. 15, 2015), available at http://europa.eu/rapid/press-release_IP-15-6321_en.htm. For a more detailed summary written for individuals whose data are protected, see the European Commission "Protection of Personal Data" web page at http://ec.europa.eu/justice/data-protection/index_en.htm.

Administrative compliance. The company must fulfill certain administrative requirements (e.g., appointment of a data protection representative) to ensure accountability and compliance with the GDPR.

Data transfers to outside the EU only with adequate safeguards. The company may transfer personal data to a place outside the EU only if there are adequate safeguards approved by the EU to ensure ongoing compliance with the rights and obligations set forth in the GDPR.

[I]—The Extent to Which the GDPR Applies to American Companies

Any American company that offers goods or services online, paid or free, or tracks online (or even offline) behavior, and that in the course of doing so processes any personal data regarding an individual located in the EU, is subject to the GDPR,[214] unless the manner in which the data are collected precludes any possibility that the person whose data are collected is located in the European Union. (The term "processed" includes collection of data from or about individuals.)[215] Even if the individuals whose data are processed are not identified, the GDPR may still apply, because its protections extend not only to identified individuals but also to "data subjects." A data subject" is defined as including not only a person identified by name, but a person who "can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[216] Thus, if the user's IP address, or the user's e-mail address if provided, or any other information provided by that user could, if looked at by a human being or analyzed by data matching, indicate that the user is located in Europe and could be identified, then the GDPR applies.

There is no specific list of items that constitute "personal data," since the definition of "personal data" is *contextual*—that is, some types of information that could be used to identify an individual in one context might not be usable to identify an individual in another context. The following is about as close as one can come to a definitive list:

- name, address in Europe, e-mail address with a European country code domain name.
- biometric data unless sufficiently anonymized so as to be useless for identification purposes.
- enough aggregate data about a person's physical, psychological, genetic, economic, sexual, cultural, racial, religious, geolocational, etc. characteristics that, taken together, will make it fairly easy to figure out who the person is.

Is an IP address that resolves to a location in Europe personal data? Are cookies? Not necessarily. Again, it *depends on the context.* The actual GDPR text never refers to "cookie" or "IP address." Those terms appear only in the preamble: "Natural persons ***may*** be associated with online identifiers . . . such as internet protocol addresses [or] cookie identifiers . . . . This ***may*** leave traces which, in particular ***when combined with unique identifiers and other information*** received by the servers, ***may*** be used to create profiles of the natural persons and identify them."[217] For an Internet service provider, an IP address in

---

[214] Art. 3(2).

[215] Art. 4(2).

[216] Art. 4(1).

[217] GDPR, Preamble, ¶ 30. (Emphasis added.)

Europe is personal data if the provider can match IP addresses with customer names. For a provider that has no ability to use a customer's IP address to find out personal information, an IP address is not personal data. Session cookies are generally not considered to be personal data but persistent cookies could be, again depending on context.[218]

Significantly, this contextual definition also applies whenever one company passes information along to another. If the receiving company can combine the sending company's information with other data so as to identify a person in Europe, then the resultant information becomes personal data even if the information components, held separately, would not be. Result: Even if neither company had to comply with the GDPR regarding the separately held data, now both companies must comply.

What about user-posted content?

Users of online forums constantly post facial images and other content that identifies European persons. Does such user-generated content (UGC) constitute Personal data? The answer is no—none of the privacy rights granted by the GDPR apply to UGC—for two reasons: First, merely by allowing UGC, the provider is not a "controller" or a "processor," and the GDPR's extensive regulations are targeted only at controllers or processors (as discussed below). A controller "***determines the purposes*** and means of the processing of personal data." A "processor" processes personal data on behalf of a controller.[219] Because an online forum provider does not even know whether personal information about European persons will be posted, and does not determine the purposes for any particular post, the provider is not a controller and thus cannot be a processor. Personal information a European user discloses administratively to an online provider such as name and address is "personal data" (Personal data). Regarding such data, the provider is a "controller," the user is a "data subject," and all his or her privacy rights under the GDPR, and all the privacy obligations of the provider, apply.[220] For example, the provider has to obtain opt-in consent from the user when collecting such data, and the user has the right to withdraw consent at any time and force the provider to delete it. But if that same user posts something online—a video, photo, comments, etc., that content is not "personal data," the user is not a "data subject" regarding it, the provider is not a "controller" regarding it, and the user has no GDPR privacy rights regarding it. It was publicly posted at the user's initiative, not administratively disclosed

---

[218] While acknowledging that the term "cookie" does not appear in the GDPR, various European authorities continue to provide their own (usually strict) interpretations regarding cookies and related technologies. The U.K., via its "Guidance on the use of cookies and similar technologies" (Information Commissioner's Office, July 3, 2019, p. 8, states: "[I]f you use cookies you must say what cookies will be set; explain what the cookies will do; and obtain consent to store cookies on devices." The French data protection authority CNIL published similar guidance. CNIL1920776Z, JORF nr. 0166, July 19, 2019. Neither authory provides guidance as to how to comply, and compliance by non-EU companies with non-EU-localized websites has been sporadic. The European Commission has proposed but not yet implemented an ePrivacy Regulation to replace the old Privacy Directive and complement the GDPR. In the meantime, the Court of Justice of the European Union (CJEU) has ruled that online pre-checked boxes indicating user consent to cookies are not enough; there must be "active" consent – and that consent is only valid if it is given after full disclosure of "clear and comprehensive" information about all aspects of cookie use: their duration, their access by third parties, the purposes for which they could be used. Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH (C-673/17, Oct. 1, 2019). Thus, the cookie-consent pop-ups that everyone, including Europeans, find irritating will continue and likely increase. No decision has yet held that companies without a presence in the EU – especially U.S. companies that comply with the Privacy Shield discussed below – must comply with the CJEU cookie decision.

[219] See definitions below.

[220] The CJEU has ruled that placing a Facebook "like" button on one's website makes one a "joint controller" Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (C-40/17, July 29, 2019). No decision has addressed whether this decision is applicable to companies without a presence in the EU – especially U.S. companies that comply with the Privacy Shield discussed below.

because the provider asked for it. This is true even if the users posts online, as UGC, the exact same information he or she disclosed administratively to the provider.

Second, under the GDPR, hosting providers are immunized from liability for UGC in almost exactly the same way the CDA and DMCA[221] immunize providers in the U.S. The immunity provision is not in the GDPR itself. Rather, the GDPR refers to another European regulation, the eCommerce Directive,[222] which contains language virtually identical to that in the DMCA: A service provider "is not liable for information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information, and . . . is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the information." As is the case for the CDA and DMCA, so to for the GDPR, a hosting company has no obligation to monitor user postings.

An online company in the U.S. that neither collects personal information about people in the EU, nor wishes to do so, can avoid being subject to the GDPR by ensuring that none of the company's data collection practices invokes GDPR jurisdiction. If all of the following statements are true,[223] the company is not subject to the GDPR:

- The company does not collect any name or address information, or if it does, will not allow the input of name information without the input of address information as well, and will not allow the input of address information indicating any address within the EU.
- The company does not collect any e-mail address information, or if it does, will not allow the input of an e-mail address with an EU country code top-level domain (ccTLD).[224]
- The company does not monitor the web browsing or app use habits of any user with an IP address that indicates that the user is located in the EU.
- The company does not allow the posting of any facial images from any IP address that indicates that the person whose image is being posted may be located in the EU.[225]
- The company does not allow any third parties that interface with its online presence (advertisers, affiliate marketers, data aggregators, etc.) to do any of the above.

There are also three categories of online companies that are exempt from the GDPR: conduits (telecommunications services), hosting services, and caching services. Article 2(4) states: "This Regulation shall be without prejudice to the application of Directive 2000/31/EC, (eCommerce Directive regarding *conduits, caching and hosting*) in particular of the liability rules of intermediary service

---

[221] Communications Decency Act § 203 and Digital Millennium Copyright Act § 512.

[222] Directive 2000/31/EC, Art. 14.

[223] One much simpler approach would be for an online company that collects personal information other than address information to include on its personal information input page a required check-box choice: "I am located in the EU: yes__ no__." Such an approach would not only enable refusing to collect any data from individuals who answer "yes," but would also make possible segregation of EU data, to which the GDPR would apply, from non-EU data.

[224] Obviously a resident of the EU could provide an e-mail address that gives no hint of EU residency; nothing in the GDPR, however, appears to provide a basis for jurisdiction over an American company that collected such an e-mail address, without more.

[225] Article 9(1) provides: "Processing of personal data revealing racial or ethnic origin, . . . and the processing of . . . biometric data for the purpose of uniquely identifying a natural person . . . shall be prohibited." Article 4(14) defines biometric data to include "facial images."

providers in Articles 12 to 15 of that Directive."[226] Article 12 of the eCommerce Directive provides that "[i]t is necessary to exclude certain activities from the scope of this Directive," and Article 43 of the Directive states: "A service provider can benefit from the exemptions for 'mere conduit' and for 'caching' when he is in no way involved with the information transmitted; this requires among other things that he does not modify the information that he transmits; this requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission.[227] Although the eCommerce Directive was intended to cover "the Internal Market" (internal-EU commerce), nothing in either the GDPR or the Directive excludes companies outside the EU that provide conduits, caching, or hosting services to the "Internal Market," and indeed, just a few lines down from Article 2(4) in the GDPR, Article 3(2) states that the GDPR "applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union. . . ."

All other American companies that process personal data regarding individuals who are in the EU are subject to the full scope of the GDPR.

[II]—The Situation Facing American Companies That Are Subject to the GDPR

The permissive American approach to online privacy and data protection. For American companies that are subject to it, the GDPR necessitates fundamental changes in the way they collect and process personal data, at least data concerning EU "data subjects."[228] Because the United States has no comprehensive privacy law, but instead has numerous *ad hoc* laws pertaining to privacy, American online companies and data analysis companies have grown accustomed to dealing with data pertaining to individuals roughly as follows:

- Any company that collects personal information must post a privacy policy and adhere to it.[229]
- A company that collects personal information can collect whatever personal data it wishes as long as it discloses its data-collection practices (usually via a link to a page entitled "your privacy is important to us"). The only constraints are the sectoral privacy laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[230] the Fair Credit Reporting Act,[231] and the Gramm-Leach-Bliley Act (GLB),[232] (banking and financial information),[233] *ad hoc*

---

[226] Emphasis added.

[227] Directive 200/31/EC, Art. 43. Although the eCommerce Directive was written in 2000, prior to the appearance of cloud providers, its wording easily applies to cloud providers, a type of hosting service, as well.

[228] American companies may choose to segregate EU personal data from U.S. personal data and comply with the GDPR only with respect to EU data, but such segregation entails implementing two sets of protective regimes where before there was only one, and with regard to EU data, compliance with the GDPR not only must apply company-wide but must also apply to all third party data processors the company deals with.

[229] The FTC, which functions as a privacy watchdog among other things, guards against unfair and deceptive trade practices such as a company's non-compliance with its own stated privacy policies.

[230] Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[231] 15 U.S.C. § 1681.

[232] 15 U.S.C. § 6801.

[233] Other such laws include the Family Education Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. § 1232g; the Cable Privacy Act, 47 U.S.C. § 551; the Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710; the Telephone Records and Privacy Protection Act, Pub. L. No. 109-476, 120 Stat. 3568; and the Restore Online Shoppers' Confidence Act of 2011 (ROSCA), Pub. L. No. 111-345, 124 Stat. 3618 (2011) (privacy of credit card billing information).

laws such as the Children's Online Privacy Protection Act (COPPA),[234] and state privacy laws, the most significant of which is the California Consumer Privacy Act (CCPA).[235]

- A company that collects personal information can use it in any way it wishes—including profiling, behavioral tracking and analysis, and data matching, and may sell or transfer the data to other companies—as long as the company's privacy policy allows it.
- A company that does not directly collect personal data but that instead processes, analyzes, stores, buys and/or sells data provided by other companies, needs to comply not with a posted privacy policy, but with sectoral privacy laws, some state privacy laws, and whatever contractual constraints may exist vis-à-vis the company's upstream data providers.
- Any company that collects data, as well as any company that processes data provided by other companies, generally can use information that is not overtly associated with any specific individual, such as an IP address or anonymized or aggregate information, in any way desired, as long as the privacy policy at the point of origin of the data collection allows it.
- Except for companies subject to sectoral privacy laws such as HIPAA and GLB, there is no obligation on the part of any company that collects or processes data to keep any records regarding what data its collects or processes, or how it uses the data, other than whatever contractual obligations may exist.
- Again with the exception of a few sectoral laws applicable to financial and medical information, etc.,[236] every company is on its own when it comes to determining how to secure its data, and how secure to keep its data.

Regarding both privacy and data protection, American law tends to focus on disclosure (privacy policies), protecting specific types of data (banking, financial, health information), and on containing the damage when data is improperly disclosed (data breach disclosure laws)[237]—something that occurs quite frequently and that often goes unremedied.[238]

The restrictive European approach to online privacy and data protection. European concepts of privacy and data protection are profoundly different from those in America. In Europe, they are based on the

---

[234] 15 U.S.C. §§ 6501-6508.

[235] The author will speak on the CCPA in an upcoming live webinar in December 2019.

[236] For example, Regulation S-P (17 C.F.R. § 248.30), promulgated pursuant to Section 504 of GLB, requires "every broker, dealer, and investment company, and every [registered] investment adviser" to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. These written policies and procedures must be reasonably designed to: (1) Insure the security and confidentiality of customer records and information; (2) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."

[237] An excellent example of the American approach is the FTC's publication "Data Breach Response: A Guide for Business" (Sept. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business.

[238] See, e.g.:
Third Circuit: Palkon v. Holmes, No. 2:14-CV-01234 SRC, 2014 WL 5341880 (D.N.J. Oct. 20, 2014) (sensitive data for more than 600,000 hotel and resort customers stolen; shareholder derivative suit dismissed).
Ninth Circuit: In re Anthem, Inc. Data Breach Litigation, 162 F. Supp.3d 953, 977 (N.D. Cal. 2016) (In a class action lawsuit against numerous health care providers, the court dismissed numerous claims as not stating causes of action under various state laws, including the lack of a private right of action: "Indiana's data breach statutes continue to provide a single enforcement mechanism: an action brought by the state Attorney General").
District of Columbia Circuit: In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation, 45 F. Supp.3d 14 (D.D.C. 2014) (in data breach complaint involving 4.7 million members of the U.S. military and their families, court held that plaintiffs whose data were stolen had no standing based on invasion of privacy, risk of identity theft, unauthorized charges to credit cards; but standing granted on other grounds: invasion of medical privacy).

belief that the privacy of personal data is a fundamental right of EU citizens. The initial "whereas" clauses of the GDPR refer to the TFEU, the constitutive document of the European Union, and state:

> (1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.
> (2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data.

The GDPR, unlike the Privacy Directive that it replaces,[239] is a comprehensive and uniform privacy and data protection regime. The GDPR is based on the following individual rights:[240]

> *Informational rights.* European persons have the right to know exactly what information about them is held, how their information is processed, for what purposes, and precisely what organizations have what information.
> *Right to data portability.* Europeans may transfer their data away from one organization and to another.
> *Right of correction.* Europeans may access and correct information that is being stored about them.
> *Right to be forgotten*. Europeans may demand that information about them be deleted when the legitimate purposes for which the data were retained no longer apply.
> *Right to be informed of data breaches.*

Any American company with a physical presence in the EU (including such "minimum contacts" as servers located in the EU that are used for processing EU personal data) must comply with it, and, if the company is actually operating within the EU, must also comply with national and local privacy laws. Significantly for American companies, the GDPR does not abrogate existing international agreements,[241] a fact that can make compliance somewhat easier, especially for larger companies that are willing to use model contractual clauses or binding corporate rules, as discussed below. American companies with no physical presence in the EU will almost certainly prefer to comply with the GDPR by participating in one such international agreement: the Privacy Shield program, also discussed below.

---

[239] Unlike Directive 95/46/EC (Privacy Directive), which, as a "Directive," required enabling laws to be passed in each of the European Union member states, and which thus resulted in a patchwork of inconsistent laws and standards, the GDPR, as a "Regulation," is directly and consistently applicable throughout the EU. Also, companies no longer have to deal with separate data protection authorities (DPAs) in each country, as was the case with the Privacy Directive; instead, a single supervisory DPA is the point of contact.

[240] Individual rights summary adapted from European Commission, "Agreement on Commission's EU data protection reform will boost Digital Single Market," Press Release (Dec. 15, 2015), available at http://europa.eu/rapid/press-release_IP-15-6321_en.htm. For a more detailed summary written for individuals whose data are protected, see "Protection of Personal Data" at http://ec.europa.eu/justice/data-protection/index_en.htm.

[241] "International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked." (Art. 96). Church-related data protection rules are also allowed to remain in effect. (Art. 91). The GDPR does contain numerous provisions allowing member states some leeway to enact additional regulations or restrictions as long as they are consistent with the GDPR.

The GDPR—Substantive provisions. The GDPR begins with 173 "whereas" clauses setting forth statements of principle, followed by ninety-nine substantive articles grouped into eleven chapters:

Chapter I	(1-4)	General provisions
Chapter II	(5-11)	Principles
Chapter III	(12-23)	Rights of the data subject
Chapter IV	(24-43)	Controller and processor
Chapter V	(44-50)	Transfer of personal data to third countries or international organizations
Chapter VI	(51-59)	Independent supervisory authorities
Chapter VII	(60-76)	Cooperation and consistency
Chapter VIII	(77-84)	Remedies, liability and penalties
Chapter IX	(85-91)	Provisions relating to specific processing situations
Chapter X	(92-93)	Delegated acts and implementing acts
Chapter XI	(94-99)	Final provisions

The GDPR defines twenty-eight specific terms that must be understood to understand the regulation. They are[242] as follows:

TERM	*DEFINITION*
personal data	any information relating to [a data subject];
data subject	an identified or identifiable natural person
identifiable natural person	one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
processing	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
restriction of processing	the marking of stored personal data with the aim of limiting their processing in the future
profiling	any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal

[242] All definitions are from Article 4. The GDPR does not capitalize the defined terms nor does it present the definitions in alphabetical order.

personal data	any information relating to [a data subject];
	preferences, interests, reliability, behaviour, location or movements
pseudonymisation	the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person
filing system	means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis
controller	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law
processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
recipient	a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing
third party	a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data
‘consent’ of the data subject	any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
personal data breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
genetic data	personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question
biometric data	personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data
data concerning health	personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status
main establishment	[relates only to controllers and processors within the EU]

personal data	any information relating to [a data subject];
representative	a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation
enterprise	a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity
group of undertakings	a controlling undertaking and its controlled undertakings
binding corporate rules	personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity
supervisory authority	an independent public authority which is established by a Member State pursuant to Article 51
supervisory authority concerned	a supervisory authority which is concerned by the processing of personal data because: (a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority
cross-border processing	(NOTE—only inner-EU)[243] [pertains only to processing that takes place by processors located in more than one Member State]
relevant and reasoned objection	an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union
information society service	a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council[244]
International organisation	an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries

Key areas of compliance for U.S. companies.

[243] So in original text, Art. 4(23).

[244] Article 4(25) note 1 provides the reference: "Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1)."

U.S. companies that are subject to the GDPR, meaning that they are "controllers"[245] or "processors," and that are not eligible for the Privacy Shield program will need to focus their compliance efforts on the following key areas:

Designation of a representative and possibly a data protection officer.

Article 27(1) requires any data processor outside the EU that is subject to the GDPR to designate in writing a representative within the EU. No particular qualifications for the representative (which may be an entity) are specified. An exception to this requirement applies to a company that only does "processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) ["personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, [or] genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"][246] or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing."[247] If a company is required to appoint a representative, the representative (alone or together with the company) is the company's point of contact for all supervisory authorities and data subjects regarding matters pertaining to the GDPR,[248] but the representative is more than the equivalent of a registered agent. The representative must maintain a detailed record of the company's processing activities.[249]

Article 37(1)(b) requires a data controller to designate a "data protection officer" whenever, among other things, "the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale." Unlike a company's representative, a data protection

---

[245] The EU Court of Justice has ruled that a company that places a Facebook "like" button on its website and allows the transmission of user data to Facebook as a result, is a "controller." Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV, CJEU C-40/17 (29 July 2019). The case applied the meaning of "controller" under the Data Protection Direcive 95/46/EC, not the GDPR, but arguably applies to the GDPR since the defnitions are identical.

[246] Articles 9(1) and 9(2) prohibit the collection of such data without the data subject's explicit consent to the collection for specified purposes.

[247] Art. 27(2).

[248] Art. 27(4).

[249] Article 30(1) states, "That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1) [transfers 'necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request'], the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1) [security of processing]." Article 31(2) contains similar requirements for processor representatives.

officer must be "designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices. . . ."[250]

Restrictions on data collection and processing.

Article 5(1) states:

"Personal data shall be (a) processed[251] lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; . . . (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; . . . ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 6(1) states:

"Processing shall be lawful only if and to the extent that at least one of the following applies:

"(a) the data subject has given consent[252] to the processing of his or her personal data for one or more specific purposes;

"(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

"(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

"(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

"(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

"(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

Article 6(4) continues:

"Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent . . . , the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, *inter alia:*

---

[250] Art. 37(5).

[251] By definition, "processing" includes collection. Art. 4(2).

[252] Although the numerous disclosures described here are required for consent to be valid, nothing in the GDPR prohibits an online company from offering an incentive or reward if consent is given.

"(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
"(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
"(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9 [discussed below], or whether personal data related to criminal convictions and offences are processed, . . .
"(d) the possible consequences of the intended further processing for data subjects;
"(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation."

Disclosure requirements when data are collected. The GDPR contains extensive disclosure requirements:[253] Article 13(1) states:

"Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

"(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
"(b) the contact details of the data protection officer, where applicable;
"(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
"(d) where the processing is based on point (f) of Article 6(1),[254] the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47 [transfers, with adequate safeguards, to a non-EU country or international organisation], or the second subparagraph of Article 49(1) [transfers to a non-EU country or international organisation without adequate safeguards], reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available."

Article 13(2) continues:

" In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

---

[253] Article 14(5) contains limited exceptions for situations where providing such information is impossible, would involve a disproportionate effort, or where there is a professional obligation of secrecy under EU or Member State (but apparently not foreign) law.

[254] "[Where] processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

> “(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
> “(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
> “(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2) [consent of the data subject], the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
> “(d) the right to lodge a complaint with a supervisory authority;
> “(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
> “(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.”

Article 14 contains disclosure requirements that apply “where personal data have not been obtained from the data subject,” that is, where the data have been obtained from a third party, or where the identity of the person could be ascertained in some way by using data obtained. Article 14(1) states:

> “Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:
>
> “(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
> “(b) the contact details of the data protection officer, where applicable;
> “(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
> “(d) the categories of personal data concerned;
> “(e) the recipients or categories of recipients of the personal data, if any;
> “(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.”

Article 14(2) continues:

> “In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:
>
> “(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
> “(b) where the processing is based on point (f) of Article 6(1) [processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require

protection of personal data, in particular where the data subject is a child], the legitimate interests pursued by the controller or by a third party;
"(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
"(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2) [consent of the data subject], the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
"(e) the right to lodge a complaint with a supervisory authority;
"(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
"(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Actions in support of data subject rights.

Articles 15 through 22: The "privacy bill of rights." Articles 15 through 22 are where the GDPR differs most significantly from American privacy and data protection law. They set forth the individually enforceable rights of every data subject in the EU:

- Right of access to information about oneself
- Right to rectification of any such information that is inaccurate or incomplete
- Right to be forgotten
- Right to restrict processing of one's personal data
- Right to stop the processing of one's personal data
- Right to data portability
- Right not to be subject to automated decision-making that has legal effects

Article 15 provides the data subject's *right of access to information*. It is quite detailed:[255]

"The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

"(a) the purposes of the processing;
"(b) the categories of personal data concerned;
"(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
"(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

[255] Compliance can be onerous. One European journalist filed an Article 15 request with an online dating site she had used, and received an 800-page response. Duportail, "I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets," The Guardian (Sept. 26, 2017).

"(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
"(f) the right to lodge a complaint with a supervisory authority;
"(g) where the personal data are not collected from the data subject, any available information as to their source;
"(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."

Article 16, the "Right to rectification," gives the data subject the right to have a controller correct or complete inaccurate or incomplete information held about him or her.

Article 17 is titled "Right to be erasure ('right to be forgotten')."[201] The first paragraph sets forth the right, the second paragraph imposes administrative requirements, and the third paragraph contains a number of exceptions:

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay . . . where one of the following grounds applies:
"(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
"(b) the data subject withdraws [the] consent on which the processing is based . . . , and where there is no other legal ground for the processing;
"(c) the data subject objects to the processing pursuant to Article 21(1) *[fundamental rights and freedoms, especially if the data subject is a child]* and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) *[any data used for direct marketing]*;
"(d) the personal data have been unlawfully processed;
"(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
"(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

"2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
"3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
"(a) for exercising the right of freedom of expression and information;

---

[201] Not to be confused with the European Court of Justice's 2014 "right to be forgotten" decision regarding search engine results, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12 (ECJ May 13, 2014) (discussed at § 11.03[3][b][ii][C] *supra*). The *Google Spain* case pertains to search engine results pointing to data about a person but not the actual data; the GDPR "right to be forgotten" pertains to the actual data, whether online or not.

"(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
"(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
"(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
"(e) for the establishment, exercise or defence of legal claims."

Article 18, "Right to restriction of processing," sets forth the circumstances under which a data subject may require a controller to restrict processing of personal data:

"1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
"(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
"(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
"(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
"(d) the data subject has objected to processing pursuant to Article 21(1) *[fundamental rights and freedoms, especially if the data subject is a child]* pending the verification whether the legitimate grounds of the controller override those of the data subject.

"2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.
"3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted."

Article 19, "Notification obligation regarding rectification or erasure of personal data or restriction of processing," requires that the controller notify the data subject when it does those things.

Article 20 is the "Right to data portability." It states:

"1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller . . . , where:
"(a) the processing is based on consent . . . or on a contract . . . ; and
"(b) the processing is carried out by automated means."

Article 21, "Right to object," states:

"1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1) *[fundamental rights and freedoms, especially if the data subject is a child]*, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
"2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
"3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
"4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
"***
"6. Where personal data are processed for scientific or historical research purposes or statistical purposes . . . , the data subject . . . shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest."

Finally Article 22, entitled "Automated individual decision-making, including profiling," states in paragraph 1: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." The remainder of Article 22 describes exceptions.

Data security. Many different provisions in the GDPR address data security. Article 24 requires all data controllers to take "appropriate technical and organisational measures" to implement "appropriate data protection policies." Article 25, titled "Data protection by design and by default," is more specific:

"1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
"2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

Article 32 continues along the same lines:

"1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including *inter alia* as appropriate:

"(a) the pseudonymisation and encryption of personal data;

"(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

"(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

"(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

"2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

Article 28(1) extends the data security requirements to third party processors: "Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."

The data security provisions authorize some alternatives for demonstrating compliance: Adherence to an "approved code of conduct" (Article 40) or an "approved certification mechanism" (Article 42).

Recording requirements—and a major exception. Article 30 contains extensive recordkeeping requirements:

"1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

"(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

"(b) the purposes of the processing;

"(c) a description of the categories of data subjects and of the categories of personal data;

"(d) the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;

"(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

"(f) where possible, the envisaged time limits for erasure of the different categories of data;

"(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1)."

Article 30(2) contains similar requirements for processors.

Article 30(5) contains a significant exception to this requirement: The recordkeeping requirements in Article 30 do not apply to a company with fewer than 250 employees "unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1)."[256]

Restrictions on transfer of data to anywhere outside the EU. An entire chapter of the GDPR, Chapter 5, deals with "transfers of personal data to third countries or international organisations." Since nearly every American company that collects or processes EU personal data intends to transfer it to, and use it in, locations other than the EU, the provisions regarding the transfer of PII outside of EU are particularly significant.

Any transfer of EU personal data to a third country such as the U.S. is illegal unless it is done pursuant to one of the specific provisions permitting it:

Express consent of the data subject.[257] Consent to collect the data, and consent to transfer it to third countries, must be given separately (and in the latter case the data subject must be warned of the potential consequences and of his or her rights). Each consent is valid only if it is freely given, specific, informed and unambiguous. The data subject can revoke consent at any time, which means that the data controller must retrieve the data subject's records for which consent was earlier given, and erase them—and must ensure that downstream companies to whom those records were disclosed will do the same. "Consent," even if given via a check box or some other more definitive way, may not always be considered to be freely given: Consent given as part of a contract of adhesion (even if fair to both sides), or consent given to an employer who could potentially fire the employee if consent is not given, might not be freely given.

Adequacy decision.[258] Article 45(1) states: "A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection." As discussed below, the Privacy Shield is available to U.S. companies on the basis of such a prior adequacy decision, and is the only such decision regarding the United States.

---

[256] "[R]acial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

[257] Arts. 4(11), 6(1), 6(4), 13(1), 13(4), and 14(2).

[258] Article 45(1) states: "A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection." As of 2017, twelve countries were the subjects of adequacy decisions. The decisions are available at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

The Privacy Shield

The Privacy Shield[259] was designed[260] to give most U.S. companies[261] an "easy" way to comply with European data protection requirements. A U.S. company can study the requirements, develop privacy, disclosure, data protection, data transfer, and response/redress policies that comply, conduct a self-assessment of these policies and of its contractual provisions regarding data transfers to third parties, decide who to name as a contact person, pay a participation fee of from $250 to $3,250 depending on annual revenue, and then certify online[262] to the Department of Commerce that it complies with the Privacy Shield Principles. As of late 2017, more than 2,500 U.S. companies had done so. Because participation in the Privacy Shield program by a U.S. company constitutes compliance with the GDPR, U.S. companies that choose to participate are in effect replacing the extensive and burdensome provisions of the GDPR with the somewhat less extensive and less burdensome provisions of the Privacy Shield.

---

[259] See generally, the European Commission Privacy Shield website: "The EU-U.S. Privacy Shield," available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

[260] Article 96 of the GDPR states: "International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked." The EU-U.S. Privacy Shield is one such agreement. Article 45(9) states: "Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC [the Privacy Directive] shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article." That provision grandfathers in the Commission Implementing Decision of July 12, 2016, the so-called "adequacy decision," that the EU-U.S. Privacy Shield provides adequate protection for EU data transferred to the U.S. The adequacy decision may be found at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL. The European Commission conducts annual reviews of the Privacy Shield. Its first annual review, "Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. privacy Shield," (COM(2017) 611 final, Oct. 18, 2017), noted that the Privacy Shield replaced the so-called "Safe Harbor" program agreed to between the U.S. and EU and that had been in effect since 2000, but that was invalidated in 2015 by Schrems v. Data Protection Commissioner, CJEU Case C-362/14 (Oct. 6, 2015). The Commission's first annual review gave the Privacy Shield a passing grade: "The annual review has demonstrated that the U.S. authorities have put in place the necessary structures and procedures to ensure the correct functioning of the Privacy Shield. The certification process has been handled in an overall satisfactory manner . . . ." *Id*., p. 4. There is also a separate (and very similar) U.S.-Swiss Privacy Shield; details can be found at https://www.privacyshield.gov. A separate arrangement called the "Umbrella Agreement" also was made to enable European criminal investigation and law enforcement agencies to transmit information to their counterparts in the United States. Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses (Sept. 8, 2015). See European Commission Statement 15/5610, "Statement by EU Commissioner Věra Jourová on the finalisation of the EU-US negotiations on the data protection 'Umbrella Agreement'" (Sept. 8, 2015). The agreement was finalized and took effect in June 2016.

[261] Only U.S. companies that are "subject to the investigatory and enforcement powers of the Federal Trade Commission, the Department of Transportation, or another statutory body" that is or will be recognized by the EU as having the power to enforce the privacy shield, are eligible to participate in the program. U.S. Dept. of Commerce, "EU-U.S. Privacy Shield Framework Principles" (July 12, 2016), p. 1, available at https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/faqs-eu-us_privacy_shield_7-16_sc_cmts.pdf. Thus, at least at the time the Privacy Shield took effect, other companies such as banks and insurance companies were not yet eligible; however, the EU may declare other sectors as eligible at any time.

[262] https://www.privacyshield.gov/PrivacyShield/ApplyNow. Participation requires a annual "cost recovery" fee ranging from $250 to $3,250 depending on the company's annual revenue.

A SUMMARY OF PRIVACY SHIELD REQUIREMENTS[263]

1) COLLECTION PRACTICES THEMSELVES: PURPOSE LIMITATION

a. The U.S. company must limit collection of personal data to that which is relevant for the purposes of the processing.

b. The U.S. company may not process personal data in a way that is incompatible with the purposes for which is the data are collected (or subsequently authorized by the EU-person.

2) NOTICE

The U.S. company must post a EuroPrivacy policy—in clear and conspicuous language when Europeans are first asked to provide personal data (or as soon thereafter as practicable, but in no event later than when the U.S. company starts using the personal data)—that includes:

a. Statement that the U.S. company participates in the Privacy Shield program and is subject to the FTC (or other U.S. authority).

b. Public commitment to comply with the Privacy Shield Principles and statement that it is subject to the FTC or other governing body so that the commitment becomes enforceable under U.S. law.

c. Link to URL of Department of Commerce Privacy Shield program website

d. List of subsidiaries that also comply with the Privacy Shield Principles

e. Information about the types of personal data collected, and purposes for which the U.S. company collects and uses it.

f. Disclosure of the type or identity of third parties to which the U.S. company discloses personal data, and the purposes for which it does so.

g. Statement of an EU-person's right to access his/her personal data.

h. Statement that the EU-person has the opportunity to opt of having his or her personal data

- disclosed to a third party (unless the third party is under a GDPR-compliant contract with the U.S. company), or
- used for a purpose materially different from that for which the personal data were originally collected or subsequently authorized, and information on how to opt out.

i. Disclosure of the choices and means the U.S. company offers EU-persons for limiting the use and disclosure of their personal data.

j. Contact information for inquiries or complaint (including EU contact information if the U.S. company has an establishment there).

k. Identification of the relevant independent dispute resolution body (and the type of body it is: a panel established by European DPAs, an ADR provider in the EU or an ADR provider in the U.S.), and link to its URL contact information for inquiries or complaints, and a statement that binding arbitration may also be available under certain conditions.

l. Statement that U.S. company may be liable when personal data are transferred to third party DCs that violate Privacy Shield Principles.

---

[263] The Privacy Shield is not a law but a bilateral agreement, and is not enforced by European data protection authorities (DPAs) but by the FTC or other governing federal agency. This list of requirements is drawn from the Feb. 23, 2016 Privacy Shield "package" transmitted by the U.S. Department of Commerce to the European Commission. The package describes the entire Privacy Shield program: The "EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce" (the "Privacy Shield Principles" or "PSPs"); Annex 1, International Trade Administration commitments; Annex 2, Department of Commerce commitments regarding the arbitral program; plus numerous letters describing safeguards in the context of intelligence gathering.

m. Statement that personal data can be disclosed to public authorities in response to lawful requests (e.g., law enforcement, national security).

3) "CHOICE" REGARDING COLLECTION PRACTICES: EU INDIVIDUALS GET TO CHOOSE

a. Any U.S. company collecting personal data must clearly and conspicuously allow EU-persons to choose (opt out) whether their personal data are
   - disclosed to a third party (other than a third party acting on behalf of the U.S. company)
   - used for a purpose materially different from that for which the data were collected (or subsequently authorized).

The EU-person need not be offered the above choice if the disclosure is to a third party acting as an agent under a GDPR-compliant contract.

b. If a U.S. company collects any "sensitive" personal data—medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information about sex life—the U.S. company must do so via affirmative opt-in if there is any chance the sensitive Euro-PII will be disclosed to a third party, or used for a purpose other than that for which it was originally collected or subsequently authorized. *NOTE—there is no exception in the Privacy Shield Principles similar to that in the previous paragraph allowing transfers to third parties as long as a contract is in place.*

c. U.S. company also must treat as "sensitive" any personal data received from a third party that the third party identifies and treats as sensitive. *(In this context third party does not mean end user.)*

4) ACCESS

U.S. company must enable the following functionality regarding all personal data it holds:

a. Allow any EU-person to access his or her personal data.

b. Allow any EU-person to correct, amend, or delete that information if it is:
   - inaccurate, or
   - has been processed in violation of Privacy Shield Principles

unless the burden/expense of providing access would be disproportionate to the risks to the EU-person's privacy in the case in question, or

unless the rights of other persons would be violated.

5) ONWARD TRANSFER ACCOUNTABILITY

a. To transfer personal data to third party "controller" U.S. company must:
   - comply with Notice and Choice
   - enter into Privacy Shield program-compliant contract with third party controller (e.g., standard contract clauses)

b. To transfer personal data to third party "agent" U.S. company must:
   - transfer the personal data only for limited and specific purposes
   - ascertain that the third party agent is obligated to provide the same level of privacy protection as the Privacy Shield Principles.
   - take reasonable and appropriate steps to ensure that the third party agent processed the personal data consistently with U.S. company's obligations under the Privacy Shield Principles.
   - upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing

- on request, provide a summary or copy of the relevant privacy provisions of its contract with the agent to the Department of Commerce.

U.S. company will remain liable if agent processes personal data inconsistently with Privacy Shield Principles unless it shows that it is not responsible for the event causing the damage.

6) SECURITY

Any U.S. company creating, maintaining, using, or disseminating personal data must take reasonable and appropriate steps to protect the data from loss and misuse, and from unauthorized access / disclosure / alteration /destruction —taking into account the risks involved in the processing and the nature of the data.

7) DATA INTEGRITY

U.S. company must take reasonable steps to ensure that Euro-PII is reliable for its intended use, accurate, complete, and current.

8) DATA RETENTION

U.S. company must comply with the Privacy Shield Principles as long as it retains personal data.

9) INDEPENDENT RECOURSE MECHANISMS

a. U.S. company must
- respond promptly to inquiries and to Department of Commerce requests for information
- respond expeditiously to complaints regarding Privacy Shield program compliance referred through Department of Commerce
- make public any Privacy Shield program report submitted to FTC if it is found to be in non-compliance with Privacy Shield Principles.

b. Complaint process:
- EU-person complains to his or her DPA.
- DPA refers complaint to Department of Commerce
- Department of Commerce attempts to address/resolve issue with U.S. company
- Department of Commerce replies to DPA within ninety days
- Claims not resolved can be arbitrated
  - Department of Commerce will adopt arbitral procedures and select arbitrators
  - Arbitration takes place under "Recourse, Enforcement and Liability" principle
  - Arbitration panel can award EU-person-specific, non-monetary equitable relief
  - No damages, costs, fees, or other remedies
  - Prior to arbitration, EU-person must raise the claimed violation directly with the U.S. company and give the U.S. company time to resolve the matter in accordance with Section III.11(d)(k) of Privacy Shield Principles; make use of the independent recourse mechanism under the Principles; and raise the issue via the EU-person's DPA and allow DPA time to transmit it to Department of Commerce.
  - Arbitration decisions are final and binding BUT a U.S. company may seek judicial review pursuant to the Federal Arbitration Act.[264]

[264] Chapter 2 of the Federal Arbitration Act ("FAA") provides that "[a]n arbitration agreement or arbitral award arising out of a legal relationship, whether contractual or not, which is considered as commercial, including a transaction, contract, or agreement described in [Section 2 of the FAA], falls under the Convention [on the Recognition and Enforcement of Foreign Arbitral Awards of June 10, 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 ("New York Convention")]." 9 U.S.C. § 202. The FAA further provides that

10) COMPLIANCE SELF-CERTIFICATION

a. Initial certification: U.S. company provides the following information:

- contact information
- activities related to personal data
- what personal data are covered by self-certification
- the URL of its personal data privacy policy
- which U.S. governing body (e.g., FTC) has jurisdiction
- any privacy program(s) the U.S. company is a member of
- method of ensuring compliance with Privacy Shield Principles (in-house, third party)
- identification of the relevant dispute resolution body
- [a couple of additional requirements re Euro-HR data if any]

b. Annual re-certification: The U.S. company must re-certify its compliance to the Department of Commerce.

11) ENFORCEMENT

U.S. law applies to all questions of interpretation and compliance with the Privacy Shield Principles and with privacy policies by U.S. companies. (Unless the U.S. company has agreed to cooperate directly with European DPAs.)[265] The Commerce Department conducts regular reviews of participating companies to ensure ongoing compliance, and the Federal Trade Commission is responsible for enforcement actions, a responsibility it takes seriously.[266]

12) POTENTIAL MEASURES TO PRECLUDE GDPR APPLICABILITY

As comprehensive and as paradigm-changing as the GDPR may be, it is not extraterritorial in scope. Thus, the only way the GDPR can apply *directly* to a U.S. company that has no presence in Europe is where the U.S. company collects "personal data" directly from "data subjects" in the EEA, for example via a website, or monitors "behaviour" of a European person (for example, by using web beacons or persistent cookies). Otherwise, the GDPR can apply to a U.S. company that has no presence in Europe only if the U.S. company signs a contract with a "controller" or "processor" that itself is subject to the GDPR, whereby the U.S. company agrees to comply with the GDPR and to subject itself to the jurisdiction of European DPAs. If the U.S. company refuses to sign such a contract, it suffers no legal penalty; rather, the GDPR simply prohibits the controller or processor from disclosing any personal data to the U.S. company.

"[a]n agreement or award arising out of such a relationship which is entirely between citizens of the United States shall be deemed not to fall under the [New York] Convention unless that relationship involves property located abroad, envisages performance or enforcement abroad, or has some other reasonable relation with one or more foreign states." *Id.* Under Chapter 2, "any party to the arbitration may apply to any court having jurisdiction under this chapter for an order confirming the award as against any other party to the arbitration. The court shall confirm the award unless it finds one of the grounds for refusal or deferral of recognition or enforcement of the award specified in the said [New York] Convention." *Id.* § 207. Chapter 2 further provides that "[t]he district courts of the United States . . . shall have original jurisdiction over . . . an action or proceeding [under the New York Convention], regardless of the amount in controversy." *Id.* § 203. (Footnote quoted directly from Annex I, p.2.).

[265] Privacy Shield program, Privacy Shield Principles, § I, ¶ 7. Because the Privacy Shield is enforced solely within the United States by U.S. government agencies under U.S. law, against U.S. companies without any presence in Europe, the GDPR provisions that permit DPAs to impose penalties of up to 20 million Euro or 4% of a company's global annual revenue *do not apply* to Privacy Shield participants. (Confirmed to the author by Department of Commerce staff.

[266] See, e.g., FTC, "Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework," press release (Sept. 7, 2017).

Some U.S. online companies with no presence in Europe have chosen to preclude GDPR liability not by complying with it, but by adding to their terms of service (which would already state that the company's home state law and U.S. federal law apply), clauses similar to the following:

> *If you use this Service, you represent and warrant that you are not a citizen of any EEA nation who is located in the EEA.*
> *NOTICE TO RESIDENTS OF EUROPEAN ECONOMIC AREA (EEA) MEMBER NATIONS:*
> *If you are a citizen of any EEA nation and are located in the EEA, you may not use the Services provided via this website.*

Such clauses should work because online companies are free to include choice-of-law provisions in online terms and conditions, specifying the applicability of local law.[267] There mere fact that a website (or app) is viewable throughout the world does not subject the website operator to foreign law.[268] Moreover, since state and federal law apply, the Computer Fraud & Abuse Act[269] also applies, and the CFAA prohibits anyone from accessing a "protected computer" without authorization. The term "protected computer" includes web servers.[270] Accordingly, if a European person merely passively views the website, U.S. state and federal law still apply. If the European person actively uses the website by entering personal data, not only is the European person violating the site's terms of service, he or she is also violating the CFAA. The fact that the European person enters personal data in violation of the U.S. site's terms of service does not switch the applicable law from U.S. to Europe, and thus does not subject the website operator to the GDPR. It is difficult to imagine how the EU could possibly hold the website operator liable for violating the GDPR under such circumstances, assuming that the U.S. operator does not ignore the prohibition and do business with users whose information indicates that they are located in the EEA.

An even simpler way to preclude GDPR liability would be to require all users who access any areas of the website that request personal information or monitor behavior to click a response to the following:

> *I am a resident of the European Economic Area (EEA)*
> *and I am currently located there: ___ YES ___ NO.*

If the person clicks "yes" he or she would get a message saying "sorry, you may not use this website." Such a clause might be preferable to the terms and conditions clauses above, since it requires an affirmative response from the user. The website operator would not even have to exclude addresses or phone numbers in the EEA since an EEA citizen who is not located in the EEA (for example, is living in the U.S.) is not protected by the GDPR and may choose to order a book or whatever and have it delivered to an address within the EEA.

---

[267] See, e.g.:
Sixth Circuit: Wong v. PartyGaming Ltd., 589 F.3d 821 (6th Cir. 2009).
Seventh Circuit: Shaw v. Hyatt International Corp., 461 F.3d 899 (7th Cir. 2006).
Eleventh Circuit: Pappas v. Kerzner International Bahamas Ltd., 585 F. App'x 962 (11th Cir. 2014).

[268] Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 433 F.3d 1199 (9th Cir. 2006).

[269] 18 U.S.C. § 1030.

[270] *First Circuit:* EF Cultural Travel B.V. v. Zefer Corp., 318 F.3d 58 (1st Cir. 2003).
Ninth Circuit: U.S. v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

The Commerce Department conducts regular reviews of participating companies to ensure ongoing compliance, and the Federal Trade Commission is responsible for enforcement actions.[271] The Privacy Shield requires that the company adopt a number of European-style privacy practices. It must limit the personal information processed to only such information as is relevant to the purpose of processing. It must carefully protect personal information and maintain strict limitations regarding transfer of personal information to third parties. It must publicly post privacy policies directed at persons in the EU, noting that it participates in the program (self-certification), and that they have certain specific rights regarding their personal data, including:

- the right to access their personal data
- the right to bring a complaint regarding use of their data directly to the business, and to have the business address and resolve the complaint at no cost to the individual
- the right to submit a complaint to a Data Protection Authority (DPA) within the EU
- the right to demand binding arbitration of any complaint that has not been otherwise resolved.[272]

EU model contractual clauses.[273] So-called model (or "standard") contractual clauses for use in data transfer contracts were approved by the Commission in 2001, 2004, and 2010 as providing adequate safeguards regarding privacy protection and are grandfathered in under Article 45(9). The clauses are extensive and contain, in contractual form, requirements equivalent to those in the GDPR itself.

EU binding corporate rules.[274] Binding corporate rules have also been around for years and are grandfathered in, but unlike the Privacy Shield and model contractual clauses, binding corporate rules require an EU sponsor, an expensive and time-consuming application and approval process by national DP authorities, annual audits and recertification, and separate approval and recertification processes for separate countries. The overall process remains overly fragmented, difficult, and subject to national requirements, which are not at all transparent. (In Belgium there must be a royal decree, for example.) Binding corporate rules are suitable, if at all, only for large multinationals. There are no standardized tools for companies to use in drafting and implementing BCRs. As of late 2017, only eighty-eight large companies had gone through the certification process. Not all EU countries recognize the BCRs of other EU countries (only twenty-four do).

---

[271] As of late 2019, the only enforcement actions undertaken by the FTC were a handful of cases where companies had falsely stated that they were Privacy Shield participants. See, e.g., FTC, "Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework," press release (Sept. 7, 2017); "FTC Takes Action against Companies Falsely Claiming Compliance with the EU-U.S. Privacy Shield, Other International Privacy Agreements," press release (June 14, 2019).

[272] U.S. Dept. of Commerce, "Fact Sheet: Overview of the EU-U.S. Privacy Shield Framework for Interested Participants" (July 12, 2016), available at https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/fact_sheet-_eu-us_privacy_shield_7-16_sc_cmts.pdf.

[273] The European Commission has issued two sets of standard contractual clauses for transfers from data controllers to data controllers established outside the EU/EEA and one set for the transfer to processors established outside the EU/EEA. The text of these pre-approved clauses is available at the European Commission web page "Model Contracts for the transfer of personal data to third countries," http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

[274] See European Commission web page, "Overview of Binding Corporate Rules," at http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm.

[I]—Other Extraterritorial Matters

The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA),[275] which prohibits, in a commercial context, the collection, use, or disclosure of personal information about Canadian residents without their consent, has been held to apply to foreign companies.[276] Canada's strict anti-spam law[277] (CASL) and the regulations promulgated thereunder[278] apply to anyone who sends a commercial electronic message[279] to any "electronic address"[280] in Canada. CASL is an opt-in law: The sender must obtain consent from the recipient before sending a commercial solicitation. The sender must provide full, valid contact information and must not use a false or misleading subject line. There are exceptions for e-mails by potential customers and responses thereto, people who know each other, transaction confirmations, safety notices, and the like.[281] An exception interesting to parties outside Canada is that the law "does not apply to a commercial electronic message . . . if the person who sends the message or causes or permits it to be sent reasonably believes the message will be accessed in a foreign state that is listed in the schedule [a list of more than 100 major countries] and the message conforms to the law of the foreign state that addresses conduct that is substantially similar to conduct prohibited under section 6 of the Act. . . ."[282]

---

[275] S.C. 2000, c. 5, ss. 2.

[276] Lawson v. Accusearch, Inc. (F.C.), 2007 FC 125, [2007] 4 F.C.R. 314 (Feb. 5, 2007), available at https://ca.vlex.com/vid/lawson-v-accusearch-inc-681787633.

[277] An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act ("CASL") (Consolidated Acts of Canada, S.C. 2010, c. 23).

[278] Electronic Commerce Protection Regulations, 81000-2-175 (SOR/DORS) ("CASL Regulations").

[279] The act covers the sending of any "electronic message," which is defined as "a message sent by any means of telecommunication, including a text, sound, voice or image message." CASL § 1.

[280] "Electronic address" is defined to mean "an address used in connection with the transmission of an electronic message to (a) an electronic mail account; (b) an instant messaging account; (c) a telephone account; or (d) any similar account." CASL § 1.

[281] CASL § 6.

[282] CASL Regulations, § 3(f).

[283] Convention on the Recognition and Enforcement of Foreign Judgments in Civil and Commercial Matters (1971).