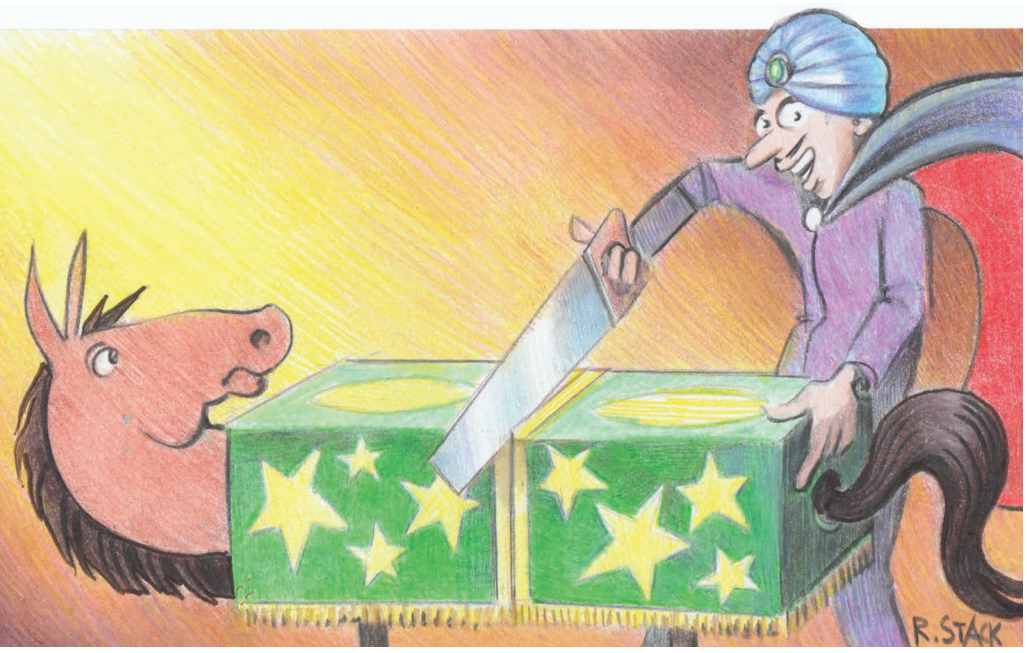
Editor: Katrine Evans, k.evans@haymanlawyers.co.nz

Microsoft v. USA: Location of Data and the Law of the Horse

Omer Tene | International Association of Privacy Professionals



The recent decision of a US Second Circuit Court of Appeals in *Microsoft v. USA*,[1] rejecting the government's attempt to compel an American company to hand over customer data stored in Ireland, appears at first glance to be a resounding victory for information privacy over government surveillance. However, at the end of the day, the case might at best be a mixed blessing for privacy advocates. By focusing attention on the intractable question that has confounded scholars for two decades—where does data "reside" on the Internet?—the decision threatens to strengthen the tide of data localization, which has little to do with preserving individual rights and further complicates the already thorny legal regime governing data protection online.

Rather than trying to capture the location of data, a concept as fickle and fleeting as Schrödinger's cat, the law—and policymakers—should focus on traditional conflict-of-laws notions, such as the location of people, organizations, and activities. While in the context of *Microsoft v. USA* such a focus might have been more intrusive to the privacy of a specific individual, overall the right to privacy would stand to gain.

What the Case Was About

On 4 December 2013, the US government served a warrant on Microsoft's headquarters in Redmond, Washington, requiring access to emails stored in the account of a customer who was suspected of drug trafficking on US soil. Despite the presence of the corporate headquarters, the suspected crime, and the law enforcement authority in the US (the suspect too might have been American, yet this isn't conclusively asserted), Microsoft refused to comply with the warrant and moved to quash, arguing that the required data was stored on servers physically located abroad.

The decision of the US Second Circuit Court of Appeals, accepting Microsoft's challenge, relied on narrow statutory grounds. Interpreting the Stored Communications Act (SCA) of 1986, the court stated, "Neither explicitly nor implicitly does the statute envision the application of its warrant provisions overseas."[1] Although that might be true, the US Congress didn't anticipate in 1986 the advent of the commercial Internet and the dawn of an era of seamless, instant, and costless transfers of data to and from the cloud. These technological developments radically changed the very nature of extraterritoriality, including cross-border application of law, on a platform that knows no territory or borders.

The *Microsoft v. USA* court ruled, "the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed—here,

 Copublished by the IEEE Computer and Reliability Societies 1540-7993/16/$33.00 © 2016 IEEE

where it is seized by Microsoft, acting as an agent of the government."[1] Yet the court's focus on the location of servers and datacenters, as opposed to the location of service providers, suspects, or crimes, isn't without doubt.

On closer scrutiny, it appears that the *Microsoft v. USA* warrant wasn't operating extraterritorially at all. Rather, a US-based employee of an American company refused to comply with a court-issued warrant concerning a crime committed on US soil on the basis that the requisite data—essentially digital zeros and ones presumably retrievable by a click of a mouse—was "located" on servers abroad. Critics might reasonably question whether the location of data—that is, ephemeral electromagnetic pulses traveling across a fiber-optic network—rather than the location of persons, companies, or crimes should be paramount. Moreover, a company's decision where to "locate" a customer's data in its networked cloud could be capricious and subject to change at any instant, undermining the stability of the legal regime.

Consider, for example, a hypothetical case, in which US law enforcement reached out to a foreign company based in France, in connection with a crime allegedly committed on French soil by a French citizen, asserting jurisdiction based on the storage of the suspect's data on servers in the US. Clearly, the interest of US law enforcement in the case would be tenuous, and its assertion of jurisdiction strained. Yet government access would likely be justified under the rationale of the *Microsoft v. USA* court, which elevates technological form over physical substance.

Judge Gerard Lynch, who filed a concurring opinion in *Microsoft v. USA*, explained that the case wasn't really about government overreach or disregard for privacy. To the contrary, "the [US] government complied with the most restrictive privacy-protecting requirements of the [SCA]. Those requirements are consistent with the highest level of protection ordinarily required by the Fourth Amendment for the issuance of search warrants."[1] Rather, the case was about the applicable law online. "The dispute here is not about privacy, but rather about the international reach of American law," wrote the judge.[1]

The court suggested that the parties draw on multilateral international solutions to untangle the web of applicable laws and regulations. Referring to Mutual Legal Assistance Treaties (MLATs), it held, "Our conclusion today also serves the interests of comity that, as the MLAT process reflects, ordinarily govern the conduct of crossboundary criminal investigations."[1] Yet critics have questioned whether MLATs are a practical tool in fast-moving criminal investigations. Stanford law professor Jennifer Granick noted, "The police would likely have to make a request through that nation's mutual legal assistance treaty provisions, which can take months."[2] And the magistrate judge in *Microsoft v. USA* observed that, "for countries with which it has not signed an MLAT, the United States has no formal tools with which to obtain assistance in conducting law enforcement searches abroad,"[1] clearly an unsatisfactory result.

The *Microsoft v. USA* decision could lead to myriad complications, and has vast implications for the heated discussion on extraterritorial application of laws governing data.

Data Localization

To be sure, the *Microsoft v. USA* court sent a clear message to US law enforcement agencies that Congress could not have intended their authority and jurisdiction to be global in nature. "We see no reason to believe that Congress intended to jettison the centuries of law requiring the issuance and performance of warrants in specified, domestic locations, or to replace the traditional warrant with a novel instrument of international application,"[1] the court held.

But by making the location of Microsoft's servers the focal point for the application of law, the court apparently reinforced the European adage that by keeping data in Europe, companies and consumers are keeping it safe, at the very least from the unwanted gaze of US law enforcement officials. This, in turn, will no doubt fuel the drive toward data localization, which has seen Europe attach strings to European-sourced data while countries such as Russia, Turkey, Brazil, and China impose even tighter restrictions.

Unfortunately, far from reinforcing privacy and fundamental rights, governments outside Europe typically employ data localization cynically to subject their own citizenry to surveillance and censorship. As Brussels academic Christopher Kuner writes, "requiring local data storage would undermine, rather than strengthen, fundamental rights by making it easier for intelligence services to access data locally and then share them with other countries."[3] In Europe, meanwhile, critics claim that not only privacy considerations but also industrial policy and protectionism have led the drive for data localization.[4]

In a world marked by free movement of humans, capital, and labor, mandating that data stay within the geographical borders of a country is reactionary. And if data localization was intended to subvert foreign surveillance, it would also offer civil rights activists little solace, because modern intelligence agencies have the ability to peer beyond national borders into the IT infrastructure of other countries, often with *less* legal process and safeguards than those applicable to domestic

surveillance. Kuner adds, "no one should be under any illusions that legal requirements to store data locally will prevent intelligence services from gaining access to them."[3]

EU Data Protection

The *Microsoft v. USA* decision occurs in a larger policy context, one that has been of great moment over the past few years. Not only national security and law enforcement agencies but also companies ranging from multinational banks and online companies to nimble app developers now have the ability to exert influence over the privacy rights of individuals in foreign countries. Indeed, the line between government and private sector interests blurred as law enforcement agencies commissioned data from private businesses,[5] or—as revealed by Edward Snowden's disclosures—tapped directly into the data warehouses of leading online providers.[6]

As Kuner notes, "Billions of individuals use the Internet, and there is uncertainty about basic questions such as whether data protection rights apply when an individual accesses a foreign web site, and how to resolve conflicts between data protection requirements 'attaching' to data transferred internationally and the law enforcement requirements of the place to which they are transferred."[3]

In assessing the *Microsoft v. USA* ruling, it's useful to draw lessons from this additional technosocial context involving the assertion of rights in cyberspace. A central stage for this debate has been the European data protection framework, which offers protection for the rights of European citizens in an interconnected economy, involving an immeasurable volume of commercial dataflows. Over the past few years, this framework has raised intense disputes over the reach of laws beyond borders, including around novel concepts such as the "right to be forgotten" and accountability mechanisms for automated decision making.

On one hand, the court's stance in *Microsoft v. USA*, recognizing the geographical limits of law in a globalized economy, stands in stark contrast to the European data protection framework, which seeks to export fundamental rights across borders and oceans to jurisdictions with entirely different legal traditions and cultural norms. Just recently, for example, the French data protection regulator, CNIL, ordered Google to apply the European-born "right to be forgotten" to its dot.com operations in the US, where implementation of such a right is likely unconstitutional.[7] And whereas in the past, under the 1995 Data Protection Directive (DPD), European law applied primarily to data processing activities performed in the context of the activities of a business established in Europe, the new General Data Protection Regulation (GDPR) will expand its application to any business, regardless of where in the world it's based, that "monitors the behavior" of Europeans or is "offering goods or services" to them. This means, for example, that a website or mobile application offered by a company based in the US, Australia, or Japan, with little or no geographical nexus to Europe, will become subject to European data protection law if it's widely used by Europeans. When compared to the deferential approach of the Second Circuit Court, the jurisdictional reach of the European data protection regime is strikingly broad.

On the other hand, European law is similar to the *Microsoft v. USA* court in placing great legal weight on data location. This is evident particularly in the European framework's restriction on cross-border data transfers. Such transfers of data to a non-European country are prohibited unless European authorities declare the laws and practices of that country "adequate" under EU standards. Alas, two decades after the framework came into force, only a handful of countries—to external observers it might seem like a random group—have been deemed "adequate." Most notably, Europe's largest trading partners, including China, India, Brazil, Japan, and the US, aren't part of this group.

To normalize its close political, trade, and business ties with the US, which hasn't obtained the adequacy stamp of approval, Europe negotiated a *sui generis* legal Safe Harbor, which was based on corporate self-certification and enforcement by a US regulator, the Federal Trade Commission. However, the Snowden revelations about the extent of government access to data under the Safe Harbor have led the Court of Justice of the European Union (CJEU) to invalidate that framework.[9] Much more than just derailing Safe Harbor, the CJEU decision could portend the demise of every legal mechanism used to transfer data out of Europe.

It took the EU and US nearly two years of intense negotiating to erect an alternative to Safe Harbor, the Privacy Shield framework, yet this arrangement remains susceptible to legal attack. And a court challenge to an alternate data transfer mechanism, standard contractual clauses, will imminently be sent from Ireland to the CJEU. Existing adequacy determinations for transfers to other countries could also be in jeopardy, as it's doubtful that the European Commission explored government access when approving them. Indeed, a claim that the data protection laws of Argentina (deemed adequate), for example, are more robust than those of the US (not deemed adequate), is groundless on its face.

It's an open secret that there's little correlation between the resources, time, and energy spent

on compliance with European cross-border data transfer regulation and the actual privacy benefits they yield. Critics decry restrictions on cross-border data transfers as a legal fiction. Individuals and organizations transfer data outside Europe all the time. Since the very first case decided under the DPD in the CJEU in 2003, European courts and regulators have struggled to overlay the DPD's cross-border dataflow provisions on a technosocial reality characterized by ubiquitous dataflows. In that first case, *Bodil Lindqvist*, data protection regulators sought legal remedies against a Swedish churchgoer for publishing a personal webpage containing rather mundane information about her colleagues in the parish. Does such publication constitute a cross-border transfer of data to any country where a user might access the site? Does an airline passenger flying from Dublin to New York with a smartphone transfer data across borders in violation of EU law? And under the GDPR, will any website or mobile app with an interface in one of the 24 official languages of the EU, including English, Spanish, French, German, and Portuguese, be viewed as "offering of goods or services" to European consumers? Like the little Dutch boy who saved Holland, European data transfer restrictions seem quaint when faced with the ever-rising tide of global data.

Unsurprisingly, these data transfer restrictions haven't been effective. According to the results of a comprehensive survey of 600 privacy professionals by the International Association of Privacy Professionals (IAPP) and EY, more than 80 percent of companies relied on preapproved standard contractual clauses to transfer data from the EU.[10] Yet execution of these clauses, which are typically treated as a mere formality, has been rote. Despite the fact that tens if not hundreds of thousands of such contracts have been signed over the years, to date, to the best of our knowledge, not a single contract has been enforced. Similar criticism weighed down on the EU–US Safe Harbor, which—even before the Snowden revelations exposed the staggering extent of government access to data transferred under it—was reputed to be woefully underenforced. Although more robust, though also legally untested, an additional transfer mechanism, binding corporate rules, is viewed as prohibitively expensive and thus practically available to only the largest and most well-resourced multinational companies. According to the IAPP-EY survey, just 8 percent of companies with fewer than 5,000 employees saw this costly mechanism as viable.[10]

Attempting to export a legal framework wholesale, together with bits and bytes of data, is unlikely to succeed and will cause additional political and economic friction.

These examples demonstrate the challenges—some would say futility—of regulation based on data location. To be sure, it might be that Europeans have simply not yet found a method effective enough to enforce the framework's data transfer obligations. The GDPR's introduction of foreboding fines in an amount of 4 percent of annual global turnover could potentially turn that around. Yet I believe the solution isn't to devise novel legal fictions to replace Safe Harbor or standard contractual clauses. Rather policymakers should come to grips with the technological reality of a world with instantaneous, seamless dataflows.

The Need for Legal Reform

The *Microsoft v. USA* judges recognized the constant renegotiation of privacy in an age marked by dizzying technological change. "Three decades ago," Judge Susan Carney held, "international boundaries were not so routinely crossed as they are today, when service providers rely on worldwide networks of hardware to satisfy users' 21st-century demands for access and speed and their related, evolving expectations of privacy."[1] Clearly, these changes require businesses to routinely revise best practices and policymakers to proactively adapt and amend existing legislation, not least the SCA and the Electronic Communications Privacy Act (ECPA), with their arcane, byzantine, antiquated legal categories and technological distinctions. This need is urgent, asserted the concurring opinion of Judge Lynch, "to emphasize the need for congressional action to revise a badly outdated statute."[1]

As explained earlier, similar problems plague the European data protection framework. The very notion of data transfers as discrete point-to-point transactions has become outdated. With data flowing seamlessly across the web, any attempt to document the location of data and erect border controls is bound to be ineffective. Alas, instead of ushering in a new era for data regulation, the GDPR largely perpetuates the DPD's flaws, relying on bureaucratic oversight over a set of formalistic compliance measures.

But how should these laws and policies be revised? Twenty years ago, in his article "Cyberspace and the Law of the Horse," US federal court of appeals judge Frank Easterbrook questioned the need for special laws to govern the Internet.[11] Easterbrook wrote, "Lots of cases deal with sales of horses; others deal

with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows."[11] And yet law schools and bar courses don't teach the Law of the Horse, he pointed out. Property and contract law, tort, and administrative law are developed at a higher level of abstraction and applied to specific factual patterns involving horses—or financial institutions or newlyweds—as the case might be.

In thinking about applicable law online, cross-border data transfers, or privacy protection, policymakers should heed Judge Easterbrook's recommendation. Regulation based on something as fickle and transient as the location of data is bound to run into conceptual and practical difficulties. At its core, the law is intended to protect individuals and regulate organizations. In a criminal law context, the right question to ask is whether a suspect or victim of a crime, an illicit activity, or a company holding relevant information are subject to the court's jurisdiction. In the *Microsoft v. USA* case, clearly they were. Hence, the quashing of the warrant based on the location of the data relied on erratic legal grounds. In the EU data protection context, regulators should examine the activities of companies established in their jurisdiction and protect the rights of their citizens. Attempting to export a legal framework wholesale, together with bits and bytes of data, is unlikely to succeed and will inevitably cause additional political and economic friction.

For centuries, private international law, the branch of law concerning conflicts of law across international borders and jurisdictions, established rules based on the location of people, organizations, and activities. These rules should continue to govern cross-border situations in an interconnected world. To replace them with special law governing data location would effectively be to opt for a counterproductive Law of the Horse. ■

References

1. Microsoft Corporation v. United States of America (In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation), docket no. 14-2985, 2nd Cir., 14 July 2016.
2. J. Granick, "The Microsoft Ireland Case and the Future of Digital Privacy," Just Security, 18 July 2016; www.justsecurity.org/32076/microsoft-ireland-case-future-digital-privacy.
3. C. Kuner, "Requiring Local Storage of Internet Data Will Not Protect Privacy," Oxford Univ. Press blog, 6 Dec. 2013; blog.oup.com/2013/12/data-security-privacy-storage-law.
4. S. Dockery, "Data Localization Takes Off as Regulation Uncertainty Continues," *Wall Street J.*, 6 June 2016; blogs.wsj.com/riskandcompliance/2016/06/06/data-localization-takes-off-as-regulation-uncertainty-continues.
5. C.J. Hoofnagle, "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement," *29 North Carolina J. Int'l Law and Commercial Regulation 595*, 2004, pp. 1–31.
6. G. Greenwald and E. MacAskill, "NSA Prism Program Taps in to User Data of Apple, Google and Others," *Guardian*, 7 June 2013; www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
7. "CNIL Orders Google to Apply Delisting on All Domain Names of the Search Engine," CNIL press release, 12 June 2015; www.cnil.fr/fr/node/15790.
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, General Data Protection Regulation, article 3(2), OJ, 4 May 2016.
9. Maximillian Schrems v. Data Protection Comm'r, Case C-362/14, ECR, 2015; http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN.
10. *IAPP-EY Annual Privacy Governance Report 2016*, IAPP-EY, 2016; iapp.org/media/pdf/resource_center/IAPP-2016-GOVERNANCE-SURVEY-FINAL2.pdf.
11. F.H. Easterbrook, "Cyberspace and the Law of the Horse," Univ. of Chicago Law School, 1996; chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2147&context=journal_articles.

Omer Tene is vice president of research and education at the International Associate of Privacy Professionals. Contact him at otene@iapp.org.

myCS
Read your subscriptions through the myCS publications portal at **http://mycs.computer.org**