Business Horizons (2016) xxx, xxx—xxx

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

For your eyes only: U.S. technology companies, sovereign states, and the battle over data protection

Stephanie Hare [@]

Independent Scholar

KEYWORDS
Data protection;
Privacy;
National security;
U.S. technology companies;
Corporate foreign policy;
Sovereign states;
European Union;
U.S. government

Abstract Who owns an individual's electronic communications data, who should have access to it, and what can be done with it? The battle of privacy versus security is currently raging between U.S. technology companies and national security forces. U.S. technology companies are adopting corporate foreign policies to respond to sovereign states' efforts to access customer data, which could change and possibly even destroy their business models. This article discusses the struggles faced by these companies and the policies influencing the possible outcome, as will be determined in the European Union within the next few years.

1. Data protection and 'corporate foreign policy'

The battle over data protection will be fought and won over the next few years in Europe, even though this conflict opposes mainly U.S. technology companies and sovereign states worldwide. Many U.S. technology companies are increasingly responding to governments' efforts to access their customers' data by defending and even asserting themselves with a 'corporate foreign policy.' This aligns a company's commercial interests in both core and new markets with its efforts to lobby various governments and defend itself in courts across multiple jurisdictions. It has even, in some instances, led U.S. technology companies to collaborate to defeat government efforts to restrict their activities as they compete with one another (see Fort, 2015; Fort & Hare, 2011a, 2011b; Schmidt & Cohen, 2010, 2013; Skapinker, 2011).

This article sets out how U.S. technology companies will most likely triumph in the key fights ahead with sovereign states who are pursuing unilateral and often conflicting agendas when it comes to data protection, even in the so-called 'single digital market' of the European Union. It also shows how

E-mail address: sr_hare@hotmail.com
[@] Twitter: @hare_brain

0007-6813/$ — see front matter
http://dx.doi.org/10.1016/j.bushor.2016.04.002

this conflict is more than a power struggle over business models: It is preventing both U.S. technology companies and sovereign states from most effectively fighting cybercrime, terrorism, and even war with the al-Qaida and the Islamic State of Iraq and Syria (ISIS)—both of which use some of these companies' products and services to recruit members and coordinate attacks. Finally, this article argues that the resolution of this battle over data protection offers the possibility of U.S. technology companies and sovereign states working more collaboratively to tackle these greater threats to the advantage of both sides, and wider peace and prosperity for their customers and citizens.

2. The 'wicked problem' of data protection

The battle over data protection—who owns an individual's electronic communications data, who should have access to it, and what can be done with it—is the very model of a 'wicked problem' as defined by Horst W. J. Rittel and Melvin M. Webber (1973), and summarized by John C. Camillus (2008) as follows:

> Wickedness isn't a degree of difficulty. Wicked issues are different because traditional processes can't resolve them. . . .A wicked problem has innumerable causes, is tough to describe, and doesn't have a right answer. . . . Environmental degradation, terrorism, and poverty—these are classic examples of wicked problems. They're the opposite of hard but ordinary problems, which people can solve in a finite time period by applying standard techniques. Not only do conventional processes fail to tackle wicked problems, they may exacerbate situations by generating undesirable consequences.

Data protection is so thorny in part because laws and treaties are created by nation-states—or in the case of the European Union, supra-states—yet the Internet largely transcends geography and physical borders, enabling the free flow of data (except, of course, in countries whose governments restrict access to many foreign websites; BBC, 2015; San Pedro, 2015; Ungerleider, 2013). As Craig Mundie, Microsoft's former chief research and strategy officer, explained (Thornill, 2015):

> People still talk about the geopolitics of oil. But now we have to talk about the geopolitics of technology. Technology is creating a new type of interaction of a geopolitical scale and importance. . . .We are trying to retrofit a governance structure which was derived from geographic borders. But we live in a borderless world.

As EU Justice Commissioner Věra Jourová has noted, this complicates sovereign states' efforts to fight crime and terrorism: "Cybercrime has no borders, while we are closed in our national jurisdictions. We need a common approach instead of a patchwork" (Neuger, 2016).

Given the stakes, it is perhaps understandable that even the most benign governments would want to regulate data protection. However, the way that many governments are framing the problem to be solved—as an issue of privacy versus security—further makes data protection a wicked problem (Rogaway, 2015). Consider, for instance, the United Kingdom's draft Investigatory Powers Bill, which will come before both houses of parliament in summer 2016 (see Bienkov, 2015; Travis, 2015; Wakefield, 2015; Watt, Mason, & Traynor, 2015).[1] This would require that the Internet browsing history of everyone in the country be stored for a year. The UK government argues that such enhanced powers would help security services and law enforcement agencies to fight crime and terrorism by providing access, without a warrant needed, to this national web history. However, U.S. technology companies have argued that this law would also create a new set of problems and risks (Fung, 2015), as it would:

- Impose UK law on non-UK businesses by forcing them to retain data about their users' online activity, and in doing so, break the laws of other countries;
- Set a precedent for other countries, including those with repressive regimes, to impose similar requirements on technology companies; and
- Increase costs by forcing telecoms to monitor and collect information about what is on their networks to a greater degree.

For these reasons, Mark Hughes, head of security at the telecommunications company Vodafone, told a UK government panel: "I am concerned that we will perhaps solve one problem, but not necessarily in the best way, and create another cybersecurity problem" (Fung, 2015).

[1] The official text of the draft IP bill is here: https://www.gov.uk/government/publications/draft-investigatory-powers-bill

3. Somebody wins, somebody loses

While cryptographers, security experts, academics, and policymakers have long recognized the wicked problem of data protection, it became apparent to the general public in summer 2013 when former U.S. National Security Agency (NSA) contractor Edward J. Snowden revealed U.S. intelligence agencies' mass surveillance of Americans and non-Americans alike, often with U.S. technology companies' consent but sometimes without it.[2] Snowden's leaks made explicit what had previously been implicit:

- Multiple stakeholders across the globe have competing interests when it comes to electronic communications data.
- These interests cannot be reconciled, as any attempt to solve this wicked problem via legislation or court rulings would necessarily help some stakeholders while hindering or outright harming others.

The following overview of some of the stakeholders, though by no means all, involved illustrates the wicked problem of data protection.

3.1. U.S. technology companies

U.S. technology companies want to create and sell products and services in order to make as much profit as possible and increase market share, and eventually attain market dominance in core and new markets. They want governments to craft laws that enable rather than hinder their activities, and for those laws not to conflict across countries in a way that hurts their business model. Pre-Snowden, these companies arguably benefited from a closer degree of complicity with the U.S. government, which promoted their products and services as tools to further U.S. foreign policy democracy (see Ross, 2010). Post-Snowden, these companies have tried to convince their customers within and outside the United States of their independence from the U.S. government, to varying degrees of success.

3.2. Liberal democracies

Countries that have made privacy, civil liberties, and human rights part of their law and culture—albeit to varying degrees and consistency throughout their history—are considered liberal democracies. Their data sharing agreements take this into account, and include such alliances as the Five Eyes—the United States, the United Kingdom, Canada, Australia, and New Zealand (see Farrel, 2013)—and the U.S.-EU Safe Harbor agreement, which until it was invalidated in October 2015 had allowed for the transfer of EU citizens' data to U.S.-based servers (see Robinson, 2016). Post-Snowden, and with the rise of ISIS, many of these countries have ratified or are considering laws that would conflict with one another. As in the earlier example of the UK Investigatory Powers Bill, this would force U.S. technology companies to break the law in one jurisdiction in order to obey the law in another—a scenario that even some intelligence officials have admitted is undesirable. Investigative journalist Duncan Campbell (2015) agrees: ''Internet companies should not have to face 'ad hoc approaches and conflicts of law.''' Meanwhile, the EU and U.S. have been working to set new standards. In February 2016, the EU Commission and the United States agreed on a new framework for transatlantic data flows. Named the EU-U.S. Privacy Shield, it will mandate more stringent protection of Europeans' personal data by U.S. companies, and will require stronger monitoring and enforcement by the U.S. Department of Commerce and the Federal Trade Commission (European Commission, 2016).

3.3. Authoritarian regimes

The protection and promotion of privacy, civil liberties, and human rights is not as strong—and sometimes even is non-existent—in the laws and cultures of countries with authoritarian regimes. Still, many of these governments and their citizenry have an appetite for the products and services made or provided by U.S. technology companies. The companies thus face a dilemma. Not entering these markets means losing out on profit, market share, and possibly global dominance. On the other hand, entering these markets may have an even higher cost in terms of being forced to compromise on data protection, as this could lead to complicity in oppression and human rights abuses, and would almost certainly make products more vulnerable to hackers and intelligence agencies.

3.4. Law enforcement and intelligence agencies everywhere

Law enforcement and intelligence agencies want laws that empower them to fulfill their mission to prevent terror attacks and other crime—or, failing

[2] For an overview of Snowden's revelations, see the Electronic Frontier Foundation (n.d.a) and the American Civil Liberties Union (n.d.). See also the Pulitzer Prize-winning coverage in *The Guardian* and *The Washington Post*; the Academy Award-winning documentary *Citizenfour*; and Taylor, Bradburn, & Thomas (2015).

that, at least to bring terrorists and criminals to justice. For those whose *raison d'être* is to serve their country and protect their fellow citizens, the fear is that encryption will allow electronic communications users to 'go dark,' hidden from state surveillance capabilities.

3.5. Individuals

Known as 'citizens' from the point of view of governments and 'customers' from the perspective of technology companies, individuals defy easy categorization. There are as many views about privacy as there are people who use electronic communications, from those who post their thoughts and actions on social media to those who eschew such platforms and encrypt their data.

3.6. Professionals who depend on data protection

Certain professionals—including journalists, human rights advocates, lawyers, and health professionals—depend on data protection to do their jobs. The chilling effect of surveillance on these professionals threatens a free press and thus democracy, the proper functioning of the market economy, and the protection of whistleblowers, attorney-client privilege, and doctor-patient confidentiality. Denying these individuals the strong data privacy they need in order to work would almost certainly lead to greater corruption, human rights abuses, and state repression—one reason why even some intelligence agents have called for greater independent oversight. According to Campbell (2015): "There must be oversight—do not assume agencies will follow the rules."

4. Privacy paradox

Is it hypocritical for millions of people to be willing to forfeit some of their privacy in exchange for U.S. technology companies' products and services, yet also feel less comfortable—if not downright appalled—by Snowden's revelations (see Rainie, 2016; Rainie & Duggan, 2016)? Not really. Researchers have long studied the concept of a privacy paradox (John, 2015). That many people are seemingly more relaxed about sharing their data with companies than governments—whether that of their own or those of other countries—reflects culture, national history, and differences in how companies and governments are empowered to use a person's data.

Sharing personal data with companies is typically low risk. Businesses can freely use personal data to manipulate and perhaps exploit consumers, but within the confines of the law cannot use it for coercive purposes.[3] By contrast, sharing personal data with governments is high risk because governments have the power to arrest, imprison, and in some cases even kill their citizens or enemies, whether secretly or in open violation of the spirit—if not the letter—of the law.

Liberal democracies, which often boast about their protection of civil liberties and chastise authoritarian regimes for failing to follow their lead, have fallen short of their own ideals here. Of the many examples that abound, Germany's post-war experience of surveillance under the Stasi in the former East is the most obvious and oft cited. Less discussed is France, which had sophisticated police surveillance systems under all its governments in the 20th century—not just the Nazi-collaborating Vichy State—and used these to monitor and control its Muslim and Jewish populations, often to deadly effect (see Blanchard, 2011; House & MacMaster, 2006). Americans, whose own experience of 20th century surveillance includes the McCarthy-era witch hunts and spying on civil rights campaigners, have grappled with cognitive dissonance post-Snowden. During the Bush administration and following the September 11th terror attacks, under Section 702 of the FISA Amendments Act (Electronic Frontier Foundation, n.d.b), government officials first admitted to gathering metadata in bulk as opposed to the content of electronic and telephone communications; later, they admitted to doing the latter, too (Electronic Frontier Foundation, 2014). The official line—that this was only a minimal intrusion and no cause for concern—was muddied in May 2014, when former NSA and CIA Director General Michael Hayden admitted (Ferran, 2014): "Metadata can tell the government 'everything' about anyone it's targeting for surveillance, often making the actual content of the communication unnecessary[4]. . . .We [the United States] kill people based on metadata."

[3] Identity theft is a risk that results from the decision to share one's data with a company, but is separate for the purposes of this discussion since it is the result of criminals breaching the company's security to steal customer data rather than the company deciding to use customer data for nefarious purposes. In this example, the company and the customers whose data have been stolen are both victims, albeit with different consequences.

[4] David Chaum (1985, p. 1038) warned about this, years before the Internet took off: "The foundation is being laid for a dossier society, in which computers could be used to infer individuals' lifestyles, habits, whereabouts, and associations from data collected in ordinary consumer transactions. Uncertainty about whether data will remain secure against abuse by those maintaining or tapping it can have a 'chilling effect,' causing people to alter their observable activities."

In the immediate aftermath of Snowden's revelations, not all of the nine U.S. technology companies named in PRISM[5], the NSA's electronic communications data-gathering program, explained themselves in ways that inspired confidence in those who had handed over their personal data in exchange for products and services (Greenwald & MacAskill, 2013). At first, most of the nine firms denied their involvement in U.S. mass surveillance and that of the UK, whose participation was revealed when Snowden provided documents on the activities of the NSA's UK counterpart, Government Communications Headquarters (GCHQ). Apple CEO Tim Cook (2016) maintains that Apple never handed over its users' data:

> I want to be absolutely clear that we have never worked with any government agency from any country to create a backdoor in any of our products or services. We have also never allowed access to our servers. And we never will.

However, some companies were soon forced to admit that they had in fact shared their customers' data.

Yahoo, whose fight against the U.S. government is in the public domain, explained the Kafkaesque world in which these companies were forced to operate. Failure to comply with the secretive Foreign Intelligence Surveillance Court (FISC) risked fines and possibly even charges of treason, as Yahoo CEO Marissa Mayer later explained[6] (Kaiser, 2013):

> If you don't comply, it is treason. We can't talk about it because it is classified. Releasing classified information is treason, and you are incarcerated. In terms of protecting our users, it makes more sense to work within the system.

To muddy the waters further, the companies were "legally indemnified against any actions arising as a result of co-operating with the authorities' requests" (Gellman & Poitras, 2013). While it is far from clear that this approach protected Yahoo's users, it did at least protect its employees from U.S. prosecution.

Amid the public outcry, many of the companies expressed outrage that the NSA had been taking data without their consent or even knowledge by harvesting it directly from fiber-optic connections. They sought to reassure and build trust by providing greater transparency about their compliance with government requests for data (Thielman, 2015a, 2015b). Several now publish transparency reports, although these are arguably of limited value because (Sayer, 2015):

- Companies can only report the number of National Security Letters or requests received under the Foreign Intelligence Service Act within broad tranches (0—999 requests, 1,000—1,999, etc.).
- They can only publish the data six months in arrears.
- The information gives no sense of the necessity and proportionality of U.S. government requests.
- In its assessment of the world's top technology companies, the New America Foundation found that all "failed to offer their users basic disclosures about privacy and censorship."

5. Digital disruption from Europe

U.S. technology companies were not alone in recognizing and seeking to limit the damage of Snowden's revelations about U.S. data mining. In June 2015, the U.S. Congress allowed the expiration of the USA Patriot Act, which had legalized the bulk collection of Americans' telephone records following the terror attacks of 9/11 (Diamond, 2015). It then passed the USA Freedom Act, which restored responsibility for those records to the telecommunications companies (MacAskill, 2015; Siddiqui, 2015).

For a brief moment, the U.S. government and U.S. technology companies were once again aligned: both sides believed that the fallout from the Snowden revelations was an American problem requiring American solutions. All it took to expose the error of this thinking was one Austrian citizen, whose victory against a Silicon Valley giant in a court based in tiny Luxembourg now threatens the business models of not only U.S. technology companies but also the transatlantic data sharing agreement upon which the operations of over 4,000 companies have relied for 15 years.

Where U.S. technology companies and the U.S. government erred was in focusing their post-Snowden

[5] The nine companies were Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, and Apple. According to the speaker's notes of the PowerPoint presentation turned over by Snowden, "98% of PRISM production is based on Yahoo, Google, and Microsoft" (Gellman & Poitras, 2013).

[6] In 2008, the Foreign Intelligence Surveillance Court of Review ruled against Yahoo, which had sued the U.S. government on the grounds that the NSA's PRISM program—which ordered the company to hand over users' email communications, not just metadata—was unconstitutional. The U.S. government threatened Yahoo with a daily fine of $250,000 during the appeal process, which the company paid until it lost that court case as well. Yahoo was legally bound from revealing the U.S. government's orders and its fight to resist them; failure to comply with this secrecy would have been punishable by imprisonment (Bell, 2014; Timburg, 2014).

responses on their U.S. audience. Congress' passage of the Protect America Act, allowing the U.S. government to collect data on targets reasonably believed to be outside of the United States without the need for individual search warrants, did little to reassure non-U.S. citizens, whose data has been mined since 2007.[7] Post-Snowden, non-U.S. citizens and governments came to see differently what had long been a reality: U.S. mass surveillance is facilitated by the 'home field advantage' acknowledged by an unnamed official in the PRISM documents. This advantage is due largely to much of the Internet's physical infrastructure being based in the United States, as is its governance through the Internet Corporation for Assigned Names and Numbers (ICANN), a not-for-profit group licensed by the U.S. Department of Commerce to issue and oversee domain names (Greenwald & MacAskill, 2013; Tett, 2016).

The U.S. home field advantage was acknowledged implicitly in 2000 by the Safe Harbor data sharing agreement. This agreement allowed companies to voluntarily sign up to self-certify their compliance with seven privacy principles meeting EU data protection standards when transferring EU citizens' data to the United States (Court of Justice of the European Union, 2015; Federal Trade Commission, 2015). However, the voluntary, self-certifying nature of Safe Harbor opened up the potential for abuse; indeed, a 2013 study found that of the 3,000 companies that elected to sign the agreement, hundreds lied and were failing to protect Europeans' data (Nielsen, 2015). That same year, the United States and the EU began negotiations to update Safe Harbor. These were fast-tracked on October 6, 2015, when the European Court of Justice (ECJ) sided with Max Schrems, an Austrian law student who argued that Snowden's revelations showed Facebook could not protect his data from NSA spying—a protection to which he is entitled under Article 8 of the EU Charter of Fundamental Rights (FRA, n.d.).

Thus, the ECJ ruling in favor of Schrems disrupted U.S. technology companies' home field advantage by shifting to the EU the locus of resolution of conflicts over data protection. This shift looks likely to solidify over the next few years, as the following examples illustrate.

5.1. Privacy shield

The United States and the EU missed the January 31, 2016, deadline to update Safe Harbor, putting more than 4,000 companies at risk of legal action for breaching EU citizens' data protection rights. However, they did manage to avoid complete legal chaos by announcing on February 2, 2016, a new data sharing agreement called Privacy Shield (European Commission, 2016; Kelion, 2015; Scott, 2016a; see also Fioretti & Volz, 2016). Before this can come into effect in April 2016, it must be approved by the 28 EU member states, and may be derailed before then by challenges from privacy activists, at least some of the member states' national data protection authorities (DPA), and the European Court of Justice. These are likely to have little confidence in the deal's purported protections, which include (Newman, 2016; Scott, 2016b):

- Written promises, to be renewed annually, from a senior U.S. director of national intelligence that U.S. intelligence agencies will avoid ''indiscriminate mass surveillance'' of EU citizens whose data is sent to the United States;
- A U.S.-based ombudsman to whom EU citizens can complain if they believe a company has not handled their data properly; and
- Verification by the U.S. Department of Commerce that businesses that sign Privacy Shield are applying EU-level data protection standards.

While Privacy Shield may not survive the next few months of legal challenges, some form of agreement over transatlantic data sharing will doubtlessly emerge—one that will do more to put EU concerns on a stronger, if not equal, footing with those of the U.S. business and intelligence community.

In the interim, U.S. technology companies will be working to comply with the EU Data Protection Reform, the two instruments of which—the General Data Protection Regulation (GDPR) and the Data Protection Directive—will come into effect in 2018 after approval from a full plenary in the European Parliament and approval by the 28 member states (European Commission, 2015b; Lomas, 2015a). Some aspects of this reform will be easier to implement than others, such as the 'right to be forgotten'—which would only apply to searches conducted within the EU—and punishing companies found to have breached privacy rules with fines of up to 4% of global turnover, amounting to billions of dollars for many U.S. technology companies (Gibbs, 2015).

More difficult to uphold will be the right of EU citizens to know when the security of their data has been compromised. This would require the fulfillment of two best-case scenarios:

[7] The Protect America Act was allowed to lapse but was then reborn in the FISA Amendments Act of 2008.

- First, that an organization holding an EU citizen's data is aware of such an incident, whether hacking from criminals or from official intelligence agencies;

- Second, that the organization complies with its duty to notify the data protection authority.

In either case, it would be difficult—if not impossible—to prove non-compliance. How would an EU citizen or a member state's data protection authority discover that a data compromise incident had occurred or if an organization had failed to report it (see Feldman, 2016)? By their very nature, cybercriminals and intelligence agencies alike strive to remain undetected when accessing data, and companies and government agencies often dislike publicizing when they have been hacked because of the further problems this can create: reputational damage, loss of consumer confidence, exhibition of IT systems weaknesses, et cetera. Even the Network and Information Security (NIS) Directive, agreed to in December 2015 but not yet ratified, does not fully address these points; it requires critical service providers to report attacks on their systems but not data breaches, and it does not apply at all to social media companies (Gardner, 2016).

5.2. Umbrella agreement

The United States and the European Union have yet to ratify a separate data sharing deal called the Umbrella agreement, which sets out how law enforcement agencies of the two entities can share data (European Commission, 2015a; Nielsen, 2015). The Act will grant EU citizens the same legal rights as U.S. citizens under the Privacy Act of 1974, thereby empowering them to sue U.S. federal agencies for data protection violations. On the U.S. side, in October 2015 the House of Representatives passed the U.S. Judicial Redress Act, which would give foreign citizens of U.S. allies the ability to sue U.S. federal agencies if their personal data is mishandled; however, the full Senate has not yet approved it (Nasr, 2016). Until it does, the European Council and the European Parliament will not sign off on their end. This creates uncertainty for U.S. technology companies.

5.3. Ireland's role in two key lawsuits

Ireland's Data Protection Authority (DPA) is expected to complete its investigation of Max Schrems' complaints by late 2016. This follows a second, late-2015, Schrems-filed lawsuit involving the DPAs of Belgium and the German city-state of Hamburg, both of which take a more hawkish view of protecting EU citizens' data (Lomas, 2015b). If Ireland's DPA decides to suspend Facebook's transatlantic data transfers, the company will have to adapt its business model, possibly by relocating its headquarters to an EU member state with stronger data protection standards. Other U.S. technology companies—which also base themselves in Ireland to take advantage of the country's low corporate tax rate, highly educated and English-speaking workforce, membership in the EU, and usage of the euro—would likely follow.

Ireland is also involved in a lawsuit that will "set a precedent. . .[of] worldwide impact," according to Gregory T. Nojeim, senior counsel for the Center for Democracy and Technology (Nakashima, 2015). The broad outlines of the case are as follows: in December 2013 a New York magistrate judge issued a search warrant in a drug-trafficking investigation, forcing Microsoft to hand over data stored in Ireland. Microsoft lost its challenge to the warrant in August 2014. Its final appeal before a three-judge panel for the U.S. Court of Appeals for the 2nd Circuit is ongoing. The Irish government supports Microsoft, although its objections to the warrant are more procedural than ideological: It argues that a mutual legal-assistance treaty exists between Ireland and the United States, so there is no need to force Microsoft to hand over the data.

A defeat for Microsoft would hurt all U.S. technology companies, because it would establish the precedent that the U.S. government can order firms to turn over their users' data, wherever in the world that data is stored. This would put U.S. technology companies at a disadvantage globally, as an individual or company wanting to keep their data safe from the U.S. government would simply switch to a non-U.S. service provider. The strategy of American cloud service providers, which have sought to reassure EU customers by storing their data in European data centers, would become useless (Khan, 2016).

5.4. Germany's data protection 'attractiveness'

Perhaps because its business model has been under pressure since the aforementioned 2013 warrant was issued, Microsoft has developed a novel counterattack to protect the data of its EU customers. The strength of this tactic, however, will only be established if it survives a U.S. legal challenge. In November 2015, Microsoft announced that it was partnering with Deutsche Telekom subsidiary T-Systems to build two new data centers in Germany, to be wholly under the control of T-Systems (Waters & Ahmed, 2015a). It is a gamble: Microsoft believes

that by having a German company own the physical buildings and control access to the data centers, data stored there will be protected from any attempts by U.S. courts to issue warrants ordering a transfer (Chazan, 2015).

Whether the Microsoft-Deutsche Telekom strategy will protect the data from U.S. surveillance is another question entirely, to say nothing of the fact that the data will be vulnerable to orders from German courts, improper handling by Deutsche Telekom—a company that in 2008 admitted to spying on its board members and journalists—and German surveillance (Chazan, 2015). Still, with International Data Corporation (2015) estimating the cloud services market to be worth as much as $70 billion in 2015, Microsoft's German alliance strategy may well prove a worthwhile experiment. Should it withstand a legal challenge, other U.S. technology companies would likely follow suit. Microsoft CEO Satya Nadella maintains that this would result in the 'tiering' of the cloud to offer different levels of protection, with customers paying more for greater privacy (Waters & Ahmed, 2015a, 2015b). In the short run, this fragmentation—also referred to as the 'splinternet' or the 'balkanization of the Internet'—would favor companies and individuals with deep pockets while hurting small-to-medium enterprises (SMEs), and thus the very entrepreneurs who so often drive innovation. It would also favor Germany and any other EU member state that chooses to privilege data protection.

6. Encryption: More than a business model

In the aforementioned examples of forthcoming legal milestones, EU member states and institutions appear fairly united in their efforts to defend against U.S. surveillance. This both compels and inspires U.S. technology companies to adapt their strategies in order to continue competing in the lucrative, 500-million-person EU market. In contrast, regarding encryption, the member states are seriously divided and the EU institutions almost sidelined. Yet, this is more challenging for U.S. technology companies, since the question of whether to weaken encryption is binary. Weakening encryption would help security services but concurrently also expose companies to greater risks of cybercrime; Keeping encryption strong would offer maximum protection against cybercrime but cripple the ability of security services and law enforcement to monitor the use of these technologies by terrorists and criminals.

In reality, the question is misleading because weakening encryption will not prevent criminals or terrorists from using electronic communications to carry out their attacks (Abelson et al., 2015). Indeed, it could actually increase their activities because backdoors will weaken the Internet as a whole. Cryptographer and security expert Bruce Schneier[8] explains (Price, 2015):

> Technically, there is no such thing as a 'backdoor to law enforcement.' Backdoor access is a technical requirement, and limiting access to law enforcement is a policy requirement. As an engineer, I cannot design a system that works differently in the presence of a particular badge or a signed piece of paper. I have two options. I can design a secure system that has no backdoor access, meaning neither criminals nor foreign intelligence agencies nor domestic police can get at the data. Or I can design a system that has backdoor access, meaning they all can. Once I have designed this less-secure system with backdoor access, I have to install some sort of policy overlay to try to ensure that only the police can get at the backdoor and only when they are authorized. I can design and build procedures and other measures intended to prevent those bad guys from getting access, but anyone who has followed all of the high-profile hacking over the past few years knows how futile that would be. There is an important principle here: We have one world and one Internet. Protecting communications means protecting them from everybody. Making communications vulnerable to one group means making them vulnerable to all. There just isn't any way around that.

Even so, sovereign states routinely call for encryption to be weakened. U.S. agencies began requesting backdoors—or the deliberate weakening of encryption—in 1985, long before Islamist jihadi groups such as al-Qaida and ISIS ushered in a new era of terrorism (Abelson et al., 2015). With every terrorist incident, these calls to weaken encryption resurface.

This poses an existential threat to U.S. technology companies' business models, something U.S. FBI Director James Comey testified to during a December 2015 Senate hearing (Dyer & Jopson, 2015):

> It's actually not a technical issue; it is a business model question. Lots of good people have designed their systems and their devices so that

[8] Schneier is a fellow at the Berkman Centre for Internet and Society at Harvard Law School, a board member of the Electronic Frontier Foundation, and author of *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (London: W. W. Norton & Company, 2015).

> judges' orders cannot be complied with for reasons I understand. I'm not questioning their motivations. The question we have to ask is, should they change their business model?

Thus far, the White House has abandoned calls for backdoors to encryption, although this could soon change; its new encryption policy is to be published shortly (Bennett, 2016). Further adding to the uncertainty, House Homeland Security Committee Chair Mike McCaul stated in December 2015 that he "planned to form a commission of tech experts, privacy advocates, NSA officials, and law enforcement officers that will devise a legislative solution within six months" (Dyer & Jopson, 2015).

EU member states are divided over the question of backdoors, with the strongest opposition coming from the Netherlands. The Dutch Ministry of Security and Justice published a letter in January 2016 acknowledging that while strong arguments could be made both for and against encryption, it favored the latter. Backdoors, the Ministry opined, would make Internet-connected technology vulnerable to "criminals, terrorists, and foreign intelligence services" (BBC, 2016). This, it contended, would "have undesirable consequences for the security of information stored and communicated and the integrity of ICT systems, which are increasingly of importance [to] the functioning of society" (BBC, 2016). France is also encryption averse. In 2015, following a horrific year of terror attacks in Paris and across the country, the French government rejected a proposed amendment to the Digital Republic Bill—itself still under consideration—that would have required all tech companies to insert backdoors into devices (Assemblée Nationale, 2016; Tung, 2016).

By contrast, Europe's loudest call for backdoors to encryption comes from the United Kingdom. This is perhaps unsurprising, given that Snowden described the UK signals intelligence agency, GCHQ, as "to all intents and purposes a subsidiary of the NSA. They [the NSA] provide technology, they provide tasking and direction as to what they [the GCHQ] should go after" (Taylor, 2015). The previous government's effort to legislate on backdoors, the Communications Data Bill, failed. However, after winning a mandate to govern alone in May 2015, Prime Minister David Cameron vowed to increase surveillance powers. His government's proposed Investigatory Powers Bill "makes explicit in law for the first time the powers of the security services and police to hack into and bug computers and phones" and "places new legal obligation on companies to assist in these operations to bypass encryption" (Travis, 2015; see also UK Government Publications, 2015).[9] Even China did not go so far when it passed a law in December 2015 compelling technology firms to aid in decrypting information, but omitting an earlier proposal requiring them to install backdoors (Blanchard, 2015).

7. Solving the 'right' problem

In response to calls to weaken encryption, Apple CEO Tim Cook said (Newcomer, 2015): "Nobody should have to decide between privacy and security. We should be smart enough to do both." This, as well as Schneier's aforestated argument, suggests that it is worth revisiting design thinking, a problem-solving methodology which asks whether we are solving the right problem (Fast Company, 2006). Is the debate over privacy versus security getting us toward the desired outcome of stopping criminals and terrorists from using U.S. technology companies' products to carry out attacks? The consensus suggests that the answer is no. Given the greater systemic risks posed by weakening encryption, many cryptographers, security experts, academics, and technology companies argue that strong encryption, which allows for privacy, also maximizes security for the digital system as a whole. By contrast, as cryptographer Phillip Rogaway explains: "When you make encryption harder to get for ordinary people, you don't deny it to terrorists. You just make the population as a whole insecure in their daily communications" (Waddell, 2015).

How, then, to reframe the question so as to solve the right problem? For instance, how can invested parties prevent criminals and terrorists from using the products and services of U.S. technology companies to do harm, while also safeguarding the encryption that is necessary for the security of the Internet? For governments, this means no longer treating these companies as adversaries and inviting them to work together on this problem—and even being willing to pay for this collaboration.

There are some signs of this already. Following the November 2015 terror attacks in Paris, French Prime Minister Manuel Valls and French Deputy Minister for Digital Affairs Axelle Lemaire met with representatives from Facebook, Twitter, Apple, Google, and Microsoft to "discuss plans to counter extremist propaganda and expand safety tools in the event of a

[9] The UK Parliamentary Science and Technology Committee (2016) criticized the bill for its lack of clarity on how encryption would be affected in its report published on February 1, 2016. See also Bienkov (2015); Wakefield (2015); and Watt, Mason, & Traynor (2015).

future attack" (Toor, 2015; see also French government, 2015). This is in line with the January 2016 meeting between U.S. intelligence agencies and Facebook, Twitter, Apple, Microsoft, and YouTube to discuss how they could work together to disrupt radicalization online (Yadron, 2016a, 2016b). That same month, Facebook also announced plans to invest €1 million in both non-governmental organizations (NGOs) countering online extremism and research into hate speech. This effort, called the Online Civil Courage Initiative and led by the Institute for Strategic Dialogue—a London-based think-tank focused on countering extremism—is "a partnership between Facebook, the Institute for Strategic Dialogue, the Amadeu Antonio Foundation, and the International Centre for the Study of Radicalisation and Political Violence" (Hook, 2016). Meanwhile, the Dutch parliament approved in December 2015 a €500,000 budget for its Ministry of Economic Affairs to support open source encryption projects (Hillenius, 2015).

U.S. technology companies, the dominance of which ensures they must play a part in any solution, too can take steps to help shift the debate away from privacy versus security. First, they must continue and even ramp up their efforts to educate and demonstrate how encryption protects the overall digital infrastructure—and thereby millions of people who and businesses which depend on it—and how backdoors would undermine this. Second, while competing against one another, these companies must also improve how they work together to lobby effectively against efforts to weaken encryption and to promote data protection, whether through open letter campaigns or via industry trade groups. Third, they must win back customers' trust by being more transparent. For example, Microsoft, Twitter, and Yahoo announced in December 2015 that they would begin notifying users if these online services were suspected targets of state-sponsored attacks. Facebook actually began the practice in October 2015 and Google has done the same since June 2012 (Wingfield, 2015). It should be a point of technology companies' corporate social responsibility to improve their current dismal performance, as evidenced by the Digital Rights Ranking.[10] Moreover, they must work to communicate to their users when and why they are prevented from revealing surveillance. This transfers some responsibility to the user, who can act in his/her capacity as a citizen to lobby the government for greater transparency.

[10] See the Ranking Digital Rights project https://rankingdigitalrights.org/ and Freedom House's Freedom on the Net rankings https://freedomhouse.org/report-types/freedom-net

U.S. technology companies will need to remain ever vigilant. They are in a stronger position when it comes to the question of whether to weaken or strengthen encryption, for the firms all oppose backdoors, while—as previously mentioned—the sovereign states remain divided. Nevertheless, sovereign states will continue to be formidable foes in this respect. In the United States, for example, technology companies joined forces with NGOs and privacy groups to protest the Cybersecurity Information Sharing Act (CISA), but were outmaneuvered at the last minute by the Senate; the legislative body included the Act with the federal budget, ensuring the Act's approval (Greenberg, 2015).

8. Conclusion

The next few years will see the resolution of several outstanding court cases and international negotiations that will shape the future of trans-Atlantic data protection, likely setting a global standard. In play are three strategies that U.S. technology companies are currently trying in order to protect their customers' data from government surveillance. First is 'encryption-at-design,' which allows the companies to make encryption a unique selling point of their products and services but is vulnerable to potential laws compelling installation of backdoors. Second is companies' attempts to safeguard customer data from U.S. court orders and U.S. surveillance by storing EU citizens' data on servers located in Europe. Third is whether U.S. technology companies can offer watertight data protection to their European customers by allying with European companies that will own and operate the data centers. The success or failure of these strategies will influence the evolution of U.S. technology firms' corporate foreign policies, likely involving closer collaboration with sovereign states. All parties should move beyond the adversarial and ultimately fruitless debate over privacy versus security, and focus instead on solving the problem of how to prevent criminals and terrorists from using these products and services for destructive ends.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., . . . Weitzner, D. J. (2015, July 6). *Keys under doormats: Mandating insecurity by requiring government access to all data communications* (Technical Report, MIT-CSAIL-TR-2015-026). Retrieved from http://www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf

American Civil Liberties Union. (n.d.) *NSA surveillance*. Retrieved January 16, 2016, from https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance

Assemblée Nationale, République Numérique (number 3318), amendment number CL92. (2016, January 4). Retrieved from http://www.assemblee-nationale.fr/14/amendements/3318/CION_LOIS/CL92.asp

BBC. (2015, December 16). *China internet: Xi Jinping calls for 'cyber sovereignty.'* Retrieved from http://www.bbc.co.uk/news/world-asia-china-35109453

BBC. (2016, January 7). *Dutch government says no to 'encryption backdoors.'* Retrieved from http://www.bbc.co.uk/news/technology-35251429

Bell, R. (2014, September 11). Shedding light on the Foreign Intelligence Surveillance Court (FISC): Court findings from our 2007—2008 Case. *Yahoo Global Public Policy.* Retrieved from http://yahoopolicy.tumblr.com/post/97238899258/shedding-light-on-the-foreign-intelligence

Bennett, C. (2016, January 13). White House poised to issue encryption policy. *The Hill*. Retrieved from http://thehill.com/policy/cybersecurity/265660-white-house-poised-to-issue-encryption-policy

Bienkov, A. (2015, June 30). David Cameron: Twitter and Facebook privacy is unsustainable. *Politics.co.uk*. Retrieved from http://www.politics.co.uk/news/2015/06/30/david-cameron-twitter-and-facebook-privacy-is-unsustainable

Blanchard, B. (2015, December 28). China passes controversial counter-terrorism law. *Reuters*. Retrieved from http://www.reuters.com/article/us-china-security-idUSKBN0UA07220151228

Blanchard, E. (2011). *La police Parisienne et les Algériens (1944—1962)*. Paris: Nouveau Monde editions.

Camillus, J. C. (2008, May). Strategy as a wicked problem. *Harvard Business Review*. Retrieved from https://hbr.org/2008/05/strategy-as-a-wicked-problem

Campbell, D. (2015, June 2). Spooks admit it in private: Snowden has made them rethink their methods. *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/2015/jun/02/spooks-snowden-transparency-mi6-gchq-cia

Chaum, D. (1985). Security without identification: Transaction systems to make Big Brother obsolete. *Communication of the ACMC, 28*(10), 1030—1044.

Chazan, G. (2015, December 7). Deutsche Telekom to offer 'secure' cloud storage out of US reach. *Financial Times*. Retrieved January 17, 2016, from http://www.ft.com/intl/cms/s/0/2b5928dc-9cca-11e5-b45d-4812f209f861.html#axzz43vRsAPeF

Cook, T. (2016). Apple's commitment to your privacy. *Apple Inc*. Retrieved from http://www.apple.com/privacy/

Court of Justice of the European Union. (2015). The Court of Justice declares that the Commission's US Safe Harbour decision is invalid [Press release No 117/15]. Retrieved from http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

Diamond, J. (2015, June 1). Patriot Act provisions have expired: What happens now? *CNN Politics*. Retrieved from http://edition.cnn.com/2015/05/30/politics/what-happens-if-the-patriot-act-provisions-expire/

Dyer, G. & Jopson, B. (2015, December 9). Encryption harms terror probes, says FBI. *Financial Times*. Retrieved from http://www.ft.com/intl/cms/s/0/76b4be00-9e9a-11e5-8ce1-f6219b685d74.html#axzz43vRsAPeF

Electronic Frontier Foundation. (2014, May 8). The way the NSA uses 702 is deeply troubling. Here's why [Web log post]. Retrieved from https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why

Electronic Frontier Foundation. (n.d.a). NSA spying on Americans [Web log post]. Retrieved from https://www.eff.org/nsa-spying

Electronic Frontier Foundation. (n.d.b). *Section 702 of the Foreign Intelligence Surveillance Act (FISA): Its illegal and unconstitutional use*. Retrieved from https://www.eff.org/document/702-one-pager-adv

European Commission. (2015a, September 8). *Questions and answers on the EU-US data protection "Umbrella agreement"* [Press release]. Retrieved from http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm

European Commission. (2015b, December 15). *Agreement on Commission's EU data protection reform will boost digital single market* [Press release]. Retrieved from http://europa.eu/rapid/press-release_IP-15-6321_en.htm

European Commission. (2016, February 2). *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield* [Press release]. Retrieved from http://europa.eu/rapid/press-release_IP-16-216_en.htm

Farrel, P. (2013, December 2). History of 5-Eyes—explainer. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer

Fast Company. (2006, March 20). *Design thinking. . .what is that?* Retrieved from http://www.fastcompany.com/919258/design-thinking-what

Federal Trade Commission. (2015). *Federal Trade Commission Enforcement of the U.S.-EU and U.S. -Swiss Safe Harbor Frameworks*. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor

Feldman, N. (2016, February 2). Europe's new 'privacy shield' looks leaky. *Bloomberg*. Retrieved from http://www.bloombergview.com/articles/2016-02-02/europe-s-new-privacy-shield-looks-leaky

Ferran, L. (2014, May 12). Ex-NSA chief: 'We kill people based on metadata.' *ABC News*. Retrieved from http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata/

Fioretti, J., & Volz, D. (2016, January 17). U.S. and EU firms warn of 'enormous' consequences if data pact talks fail. *Reuters*. Retrieved from http://www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN0UV0YR

Fort, T. L. (2015). *The diplomat in the corner office: Corporate foreign policy*. Stanford: Stanford University Press.

Fort, T. L., & Hare, S. (2011a, February). Foreign policy joins the corporate toolkit. *Oxford Analytica Daily Brief*.

Fort, T. L., & Hare, S. (2011b, April). *Work in Progress: Corporate Foreign Policy*. Paper presented to the Council on Foreign Relations in Washington D.C. (April 26, 2011) and at the Chicago Council on Global Affairs (March, 5, 2013). Retrieved January 14, 2016, from https://www.academia.edu/2092025/Corporate_Foreign_Policy.

FRA. (n.d.) *EU Charter of Fundamental Rights: Article 8 — Protection of personal data*. Retrieved from http://fra.europa.eu/en/charterpedia/article/8-protection-personal-data

French government. (2015, December 3). Réunion de travail avec les grands acteurs de l'Internet et des réseaux sociaux [Communiqué]. Retrieved from http://www.gouvernement.fr/partage/5981-reunion-de-travail-avec-les-grands-acteurs-de-l-internet-et-des-reseaux-sociaux

Fung, B. (2015, December 21). Tech companies are slamming a proposed UK terrorism law. Here's why. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2015/12/21/tech-companies-are-slamming-a-proposed-uk-terrorism-law-heres-why/

Gardner, S. (2016, January 25). EU Parliament Panel OKs network security directive. *Bloomberg Law: Privacy and Data Security*. Retrieved from http://www.bna.com/eu-parliament-panel-n57982066517

Gellman, B., & Poitras, L. (2013, June 7). US, British intelligence mining data from nine US Internet companies in broad secret program. *The Washington Post*. Retrieved from https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Gibbs, S. (2015, December 16). EU agrees draft text of pan-European data privacy rules. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2015/dec/16/eu-agrees-draft-text-pan-european-data-privacy-rules

Greenberg, A. (2015, December 16). Congress slips CISA into a budget bill that's sure to pass. *Wired*. Retrieved from http://www.wired.com/2015/12/congress-slips-cisa-into-omnibus-bill-thats-sure-to-pass/

Greenwald, G., & MacAskill, E. (2013, June 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Hillenius, G. (2015, December 10). Dutch government to shore up open source security. *European Commission*. Retrieved from https://joinup.ec.europa.eu/node/148059

Hook, L. (2016, January 18). Facebook attempts to counter extremist posts. *Financial Times*. Retrieved from http://www.ft.com/cms/s/0/ce5cf3ba-be3a-11e5-846f-79b0e3d20eaf. html#axzz3xjyTe3jS

House, J., & MacMaster, N. (2006). *Paris 1961: Algerians, state terror, and memory* (chapter 1). Oxford: Oxford University Press.

International Data Corporation. (2015, July 21). *Public cloud computing to reach nearly $70 billion worldwide, according to IDC* [Press release]. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS25797415

John, L. (2015, October 16). We say we want privacy online, but our actions say otherwise. *Harvard Business Review*. Retrieved from https://hbr.org/2015/10/we-say-we-want-privacy-online-but-our-actions-say-otherwise

Kaiser, T. (2013, September 13). Yahoo CEO Marissa Mayer feared treason for failing to comply with NSA requests. *DailyTech*. Retrieved from http://www.dailytech.com/Yahoo+CEO+Marissa+Mayer+Feared+Treason+for+Failing+to+Comply+with+NSA+Requests/article33375.htm

Kelion, L. (2015, October 6). Facebook data transfers threatened by Safe Harbor ruling. *BBC*. Retrieved from http://www.bbc.co.uk/news/technology-34442618

Khan, J. (2016, January 7). Amazon's pitch to Europe: Your data is safe from American spies. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/articles/2016-01-07/amazon-s-pitch-to-europe-your- data-is-safe-from-american-spies

Lomas, N. (2015a, December 16). Europe finally agrees tough new data protection rules. *TechCrunch*. Retrieved from http://techcrunch.com/2015/12/16/gdpr-agreed/

Lomas, N. (2015b, December 3). With no European safe harbor, Facebook faces privacy complaints on multiple fronts. *TechCrunch*. Retrieved from http://techcrunch.com/2015/12/03/schrems-steps-up-mass-surveillance- fight-against-facebook/

MacAskill, E. (2015, November 28). The NSA's bulk metadata collection authority just expired. What now? *The Guardian*. Retrieved from http://www.theguardian.com/us-news/2015/nov/28/nsa-bulk-metadata-collection-expires-usa-freedom-act

Nakashima, E. (2015, September 9). U.S. battle over Microsoft e-mails could result in 'global free-for-all.' *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/us-battle-over-microsoft-e-mails-could-result-in-global-free-for-all/2015/09/09/f8dcbf1e-5722-11e5-abe9-27d53f250b11_story.html

Nasr, A. (2016, January 13). Senate cutting it close on international data sharing. *Morning Consult*. Retrieved from https://morningconsult.com/2016/01/senate-deadline-judicial-redress-act/

Neuger, J. G. (2016, January 26). EU starts dialogue with Internet providers to probe cybercrimes. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/articles/2016-01-26/eu-starts-dialogue-with-internet-providers-to-probe-cybercrimes

Newcomer, E. (2015, October 20). Apple CEO defends encryption, opposes government backdoor. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/articles/2015-10-20/apple-ceo-defends-encryption-opposes-government-back-door

Newman, A. (2016, February 2). Transatlantic privacy shield could yet be pierced by regulators. *Financial Times*. Retrieved from http://www.ft.com/cms/s/0/f497cff6-c9a6-11e5-a8ef-ea66e967dd44. html#axzz3z2d9djKy

Nielsen, N. (2015, September 9). EU and US sign law enforcement data pact. *EUobserver*. Retrieved from https://euobserver.com/justice/130176

Price, R. (2015, July 6). Bruce Schneier: David Cameron's proposed encryption ban would 'destroy the internet.' *Business Insider*. Retrieved from http://uk.businessinsider.com/bruce-schneier-david-cameron-proposed-encryption-ban-destroy-the-internet-2015-7

Rainie, L. (2016, January 14). How Americans balance privacy concerns with sharing personal information: 5 key findings. *Pew Research Center*. Retrieved from http://www.pewresearch.org/fact-tank/2016/01/14/key-findings-privacy-information-sharing/

Rainie, L., & Duggan, M. (2016, January 14). Privacy and information sharing. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/

Rittel, H. W. J., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy Sciences, 4*(2), 155—169 Retrieved from http://www.uctc.net/mwebber/Rittel+Webber+Dilemmas+General_Theory_of_Planning.pdf

Robinson, D. (2016, February 2). EU and US reach deal on transatlantic data sharing. *Financial Times*. Retrieved from http://www.ft.com/cms/s/0/7a9954d2-c9c8-11e5-be0b-b7ece4e953a0.html#axzz3z2wxWEEY

Rogaway, P. (2015). *The moral character of cryptographic work*. Essay written to accompany the 2015 IACR Distinguished Lecture given at Asiacrypt 2015 in Auckland, New Zealand. Retrieved from http://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf

Ross, A. J. (2010, October 1). Definition of eDiplomacy [Video file]. *HUB Institute*. Retrieved from https://www.youtube.com/watch?v=OsMWA_nKkFo

San Pedro, E. (2015, August 10). Cuban internet delivered weekly by hand. *BBC*. Retrieved from http://www.bbc.co.uk/news/technology-33816655

Sayer, P. (2015, November 12). EU wants US companies to report intelligence agency data access requests. *PCWorld*. Retrieved from http://www.pcworld.com/article/3004836/eu-wants-us-companies-to-report-intelligence-agency-data-access-requests.html

Schmidt, E., & Cohen, J. (2010, November/December). The digital disruption: Connectivity and the diffusion of power. *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/articles/2010-10-16/digital-disruption

Schmidt, E., & Cohen, J. (2013). *The new digital age: Reshaping the future of people, nations and business*. London: John Murray Publishers Ltd.

Scott, M. (2016a, January 31). U.S. and Europe fail to meet deadline for data transfer deal. *The New York Times*. Retrieved from http://www.nytimes.com/2016/02/01/technology/us-european-data-transfer-deal.html

Scott, M. (2016b, February 2). U.S. and Europe in 'safe harbor' data deal, but legal fight may await. *The New York Times*. Retrieved from http://www.nytimes.com/2016/02/03/technology/us-europe-safe-harbor-data-deal.html

Siddiqui, S. (2015, June 3). Congress passes NSA surveillance reform in vindication for Snowden. *The Guardian*. Retrieved from http://www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden

Skapinker, M. (2011, October 27). Business needs a world view of its own. *Financial Times*. Retrieved from http://www.ft.com/cms/s/0/d188bdfa-fe34-11e0-a1eb-00144feabdc0.html#axzz3xua15oZl

Taylor, P. (2015, October 5). Edward Snowden interview: 'Smartphones can be taken over.' *BBC*. Retrieved from http://www.bbc.co.uk/news/uk-34444233

Taylor, P. (Reporter), Bradburn, H. (Producer), & Thomas, C. (Editor). (2015, October 9). Edward Snowden: Spies and the law [Documentary film]. *BBC One Panorama*. Retrieved from http://www.bbc.co.uk/programmes/b06h7j3b

Tett, G. (2016, January 28). Why ICANN and internet governance are no longer America's domain. *Financial Times*. Retrieved from http://www.ft.com/cms/s/0/c9ec6e58-c41d-11e5-b3b1-7b2481276e45.html#axzz3z2wxWEEY

Thielman, S. (2015a, November 3). "If this was a test, then nearly everyone failed": How tech giants deny your digital rights. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2015/nov/03/ranking-digital-rights-project-data-protection

Thielman, S. (2015b, November 3). World's biggest tech companies get failing grade on data-privacy rights. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2015/nov/03/data-protection-failure-google-facebook- ranking-digital-rights

Thornill, J. (2015, September 7). Europe is ill-equipped for borderless world of technology. *Financial Times*. Retrieved from http://www.ft.com/cms/s/0/212508ae-5576-11e5-9846-de406ccb37f2.html#axzz3xdSLlXAi

Timburg, C. (2014, September 11). U.S. threatened massive fine to force Yahoo to release data. *The Washington Post*. Retrieved from https://www.washingtonpost.com/business/technology/us-threatened-massive-fine-to-force-yahoo-to-release-data/2014/09/11/38a7f69e-39e8-11e4-9c9f-ebb47272e40e_story.html

Toor, A. (2015, December 3). France wants Facebook and Twitter to launch an 'offensive' against ISIS propaganda. *The Verge*. Retrieved from http://www.theverge.com/2015/12/3/9842258/paris-attacks-facebook-twitter-google-isis-propaganda

Travis, A. (2015, November 4). Investigatory powers bill: The key points. *The Guardian*. Retrieved from http://www.theguardian.com/world/2015/nov/04/investigatory-powers-bill-the-key-points

Tung, L. (2016, January 18). Encryption backdoors by law? France says 'non.' *ZDnet*. Retrieved from http://www.zdnet.com/article/encryption-backdoors-by-law-france-says-non/

UK Government Publications. (2015, November 4). *Draft Investigatory Powers Bill*. Retrieved from https://www.gov.uk/government/publications/draft-investigatory-powers-bill

UK Parliament Committee on Science and Technology. (2016, February 1). *Cost of Investigatory Powers Bill could undermine UK Tech sector*. Retrieved from http://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news-parliament-2015/investigatory-powers-bill-report-published-15-16/

Ungerleider, N. (2013, May 14). Iran's "Halal Internet" is really a "Filternet." *Fast Company*. Retrieved from http://www.fastcompany.com/3009714/irans-halal-internet-is-really-a-filternet

Waddell, K. (2015, December 11). The moral failure of computer scientists. *The Atlantic*. Retrieved http://www.theatlantic.com/technology/archive/2015/12/the-moral-failure-of-computer-science/420012/

Wakefield, J. (2015, January 13). Can the government ban encryption? *BBC*. Retrieved from http://www.bbc.co.uk/news/technology-30794953

Waters, R. & Ahmed, M. (2015a, November 12). Microsoft's Satya Nadella rethinks the cloud. *Financial Times*. Retrieved January 16, 2016, from http://www.ft.com/cms/s/0/bd768884-88e0-11e5-90de-f44762bf9896.html#axzz3xdSLlXAi

Waters, R. & Ahmed, M. (2015b, November 11). US cloud blows over Atlantic to find protection. *Financial Times*. Retrieved from http://www.ft.com/cms/s/0/da408a76-8892-11e5-90de-f44762bf9896.html#axzz3xdSLlXAi

Watt, N., Mason, R., & Traynor, I. (2015, January 12). David Cameron pledges anti-terror law for internet after Paris attacks. *The Guardian*. Retrieved from http://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet- paris-attacks-nick-clegg

Wingfield, N. (2015, December 31). Microsoft to notify users of government hackings. *New York Times*. Retrieved from http://www.nytimes.com/2016/01/01/technology/microsoft-to-notify-users-of-government-hackings.html?_r=0

Yadron, D. (2016a, January 7). Agenda for White House summit with Silicon Valley. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2016/jan/07/white-house-summit-silicon-valley-tech- summit-agenda-terrorism

Yadron, D. (2016b, January 7). Revealed: White House seeks to enlist Silicon Valley to 'disrupt radicalization.' *The Guardian*. Retrieved from http://www.theguardian.com/technology/2016/jan/07/white-house-social-media-terrorism-meeting- facebook-apple-youtube-