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