ARTICLE

DIGITAL SWITZERLANDS

KRISTEN E. EICHENSEHR†

U.S. technology companies are increasingly standing as competing power centers that challenge the primacy of governments. This power brings with it the capacity to bolster or undermine governmental authority, as well as increasing public demands for the companies to protect users from governments. The companies' power raises serious questions about how to understand their role. Scholars have proposed varying conceptions, suggesting that the companies should be understood as public utilities, information fiduciaries, surveillance intermediaries, or speech governors. This Article takes up another possibility, one suggested by the companies themselves: that they are "Digital Switzerlands."

The Digital Switzerlands concept encompasses two ideas: (1) that the companies are on par with, not subordinate to, the countries that try to regulate them, and (2) that they are, in some sense, neutral. This Article critically evaluates the plausibility of these claims and explores how the companies differ from other powerful private parties. The Digital Switzerlands concept sheds light on why the companies have begun to resist both the U.S. government and foreign governments, but it also means that the companies do not always counter governments. Understanding the relationship between companies, users, and governments as triangular, not purely hierarchical,

* This Article reflects developments through February 2019, when it was finalized for publication.

† Assistant Professor, UCLA School of Law. For helpful conversations and comments, I am grateful to Asli Bâli, Yochai Benkler, Eyal Benvenisti, Sam Bray, Arturo Carrillo, Zach Clopton, Jennifer Daskal, Laura Dickinson, Michael Dorf, David Fontana, Maggie Gardner, Jennifer Granick, James Grimmelmann, Oona Hathaway, Chris Hoofnagle, Sung Hui Kim, Sarah Kreps, Máximo Langer, Odette Lienau, Herb Lin, Jon Michaels, Sean Murphy, Neil Netanel, Ted Parson, Sabeel Rahman, Kal Raustiala, Richard Re, Sid Tarrow, Jonathan Zittrain, and participants in workshops at the American Academy of Arts and Sciences, AALS National Security Law Section, ASIL Midyear Research Forum, Cornell Law School, Georgetown University Law Center, George Washington University Law School, Penn State Law, Stanford Center for International Security and Cooperation, UC Berkeley Center for Long-Term Cybersecurity, UCLA School of Law, and Vanderbilt Law School. Thanks to Andrew Brown, Ariel Cohen, Nick Garver, Danielle Hesse, Vincent Marchetta, and Josh Ostrer for excellent research assistance.

reveals how alliances among them affect the companies' behavior toward governments. But the companies' efforts to maintain a posture of neutrality also carry a risk of passivity that may allow governmental attacks on users to go unchallenged.

Turning to the normative, this Article proposes several considerations for assessing the desirability of having companies be Digital Switzerlands. Does the rise of the companies as competing power centers benefit individual users? Does the companies' lack of democratic attributes render them illegitimate powers? If the companies claim the benefits of the sovereign analogy, should they also be held to the public-law values imposed on governments, and if so, how? And if there is value in the companies acting as Digital Switzerlands, how can this role be entrenched to prevent backsliding? This Article offers preliminary answers to these questions, while acknowledging that the answers may well evolve along with the companies' behavior.

INTRODUCTION

In a recent speech, Microsoft President Brad Smith argued that technology companies collectively need to become a "Digital Switzerland."[1] This striking claim put a label on the emerging reality that although somewhat bounded by the laws of the countries in which they are

1 Brad Smith, President, Microsoft Corp., Keynote Address at the RSA Conference 2017: The Need for a Digital Geneva Convention 12 (Feb. 14, 2017) (transcript available at https://blogs.microsoft.com/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf [https://perma.cc/GKB5-SCUF]).

headquartered or operate, U.S. technology companies are increasingly standing as competing power centers, challenging the primacy of governments. This power brings with it significant capacity to bolster or undermine governmental authority and increasing public demands for the companies to take action to protect users from governments. It has become de rigueur to attack the companies for doing both too much and too little.[2]

Major U.S. technology companies in recent years have undergone a dramatic evolution.[3] Companies like Yahoo and Google were once—not terribly long ago—criticized for complicity with foreign governments' human rights abuses. But since that time, the companies shifted first to challenging the actions and policies of foreign governments. Then, in the wake of the Snowden disclosures, they shifted again, expanding their mandate to countering all governments, prominently including the United States, at least sometimes. The Digital Switzerland idea embodies the latest, tentative step in the evolution—a shift from simply blocking and checking governments to providing an affirmative theory of the companies' role in the digital ecosystem and in international affairs. To be sure, these are not the first superempowered private parties, but they differ in some salient ways from other powerful private actors, both historical and contemporary, in ways that affect the feasibility of their claim to be Digital Switzerlands.[4] They

2 *See, e.g.*, FRANKLIN FOER, WORLD WITHOUT MIND: THE EXISTENTIAL THREAT OF BIG TECH 192 (2017) ("The threat of bigness posed by Amazon, Facebook, and Google is a threat to self-government."); K. Sabeel Rahman, *The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept*, 39 CARDOZO L. REV. 1621, 1672 (2018) ("The threat that such private control poses to our larger political, economic, and social life . . . arises from the increasingly essential status in our internet economy, and the myriad of ways in which the platforms can be manipulated to operate on unequal, discriminatory, or misleading terms."); David Streitfeld, *Tech Giants, Once Seen as Saviors, Are Now Viewed as Threats*, N.Y. TIMES (Oct. 12, 2017), https://www.nytimes.com/2017/10/12/technology/tech-giants-threats.html (noting that the U.S. tech companies' "amount of concentrated authority resembles the divine right of kings, and is sparking a backlash that is still gathering force"); Nitasha Tiku, *How Big Tech Became a Bipartisan Whipping Boy*, WIRED (Oct. 23, 2017, 7:00 AM), https://www.wired.com/story/how-big-tech-became-a-bipartisan-whipping-boy [https://perma.cc/CN8P-9Y35] ("[C]alls to rein in Silicon Valley superpowers are coming from all parts of the political spectrum, from people who agree on little else."); Craig Timberg, Hamza Shaban & Elizabeth Dwoskin, *Fiery Exchanges on Capitol Hill as Lawmakers Scold Facebook, Google and Twitter*, WASH. POST (Nov. 1, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/11/01/fiery-exchanges-on-capitol-hill-as-lawmakers-scold-facebook-google-and-twitter [https://perma.cc/4YJU-KA72] (quoting Senator Dianne Feinstein as saying, while remonstrating tech company executives about their handling of Russian interference in the 2016 election, "You bear this responsibility. You've created these platforms. And now they are being misused. And you have to be the ones to do something about it. Or we will."). *But see* Emily Parker, Opinion, *Silicon Valley Can't Destroy Democracy Without Our Help*, N.Y. TIMES (Nov. 2, 2017), https://www.nytimes.com/2017/11/02/opinion/silicon-valley-democracy-russia.html ("It has become popular to demonize Silicon Valley.").

3 *See infra* notes 77–79 and accompanying text (discussing limitation to U.S. and Western European companies).

4 *See infra* Section I.C. While Smith used "Digital Switzerland" singular, this Article uses "Digital Switzerlands" plural in recognition of the fact that the tech companies are less like Swiss cantons, unified in a single country, than like independent but similarly acting neutral states. Their differing business

aspire to be global, not national. They have global *users*, not just customers or shareholders. And they are attractive, not extractive, drawing on soft power rather than hard power.

Embedded in the companies' undoubtedly self-interested assertion of Digital Switzerlands status are two claims. First, labeling technology companies as "Digital Switzerlands" suggests that they are on par with, not subordinate to, governments, including those governments that try to regulate them. It is, in essence, the idea that they have become supplemental sovereigns, governing individuals alongside states. Second, the choice of Switzerland, out of all possible countries, as the companies' analytic parallel highlights that they aim to be, in some sense, neutral.

In useful ways, the Digital Switzerland analogy has purchase. On the parity point, analogizing to Switzerland may be aiming low: the companies have transnational reach, many have user bases rivaling the population of China, and some have financial resources that outstrip Switzerland itself, to say nothing of less well-off countries. The companies also exhibit a mixture of motives—interests versus ideals—that are on full display in states too. On the goal of neutrality, some of the companies' recent arguments in legal proceedings and in public echo well-established principles from the international law of neutrality, including that neutrals cannot differentially support parties to a conflict and that parties to a conflict have an obligation not to target or use facilities in neutral states.

But in other salient ways, the analogy runs out. Most obviously, the companies lack territory, statehood, and sovereignty—key features of countries. And countries by and large do not recognize the companies as fellow Westphalian entities.[5] Moreover, neutrality is a complicated posture. Despite their efforts to appear neutral, the companies remain strongly associated with the United States, where they are headquartered, and subject to compulsion wherever they operate. Their attempts to remain neutral also carry with them a risk of passivity that can allow governmental attacks on users to go unchallenged. Understanding the relationship between U.S. technology companies, users, and governments as triangular, not purely

models and cultures lead to somewhat differing conceptions of neutrality and raise different issues. For example, the controversy over Russian exploitation of social media networks and ad purchases has pulled in Facebook, Twitter, and Google, *see infra* notes 222–25 and accompanying text, but not Apple, whose business model doesn't depend on targeted advertising in the same way. Interestingly, at least one report indicates that Google previously used the idea of a "digital Switzerland" in a different context. *See* KEN AULETTA, GOOGLED: THE END OF THE WORLD AS WE KNOW IT 5 (2009) (describing a meeting in which Google CEO Eric Schmidt and cofounder Sergey Brin "explained that Google was a digital Switzerland, a 'neutral' search engine that favored no content company and no advertisers" and whose "search results were 'objective,' based on secret algorithms").

5 *But see infra* notes 160–62 and accompanying text (discussing Denmark's appointment of an ambassador to the tech companies in Silicon Valley).

hierarchical, however, helps to reveal how alliances among the three have affected and will continue to affect the companies' behavior toward governments. Neutrality is a role into which the companies are still growing, while continuing to make significant missteps along the way.

This Article proposes key criteria to consider in assessing the desirability of companies serving as Digital Switzerlands and offers preliminary conclusions. First, the rise of the technology companies as competing power centers, challenging established sovereigns, could be construed as a positive development for individual users. The companies are a powerful force capable of challenging governmental Leviathans. Yet the companies are also another layer of power over individuals. Are individuals better or worse off as a result of the companies' role? The answer will depend on one's view of the relative prevalence of the companies' roles as regulator and shield, as well as one's level of concern about governments.

Second, the companies as supplemental sovereigns over individuals are not democratic. Users who are not shareholders lack governance rights, and it is nearly impossible for an individual not to pledge fealty to one (or more) of the technology companies. On the other hand, the allegiance is chosen, not assigned by birth, like citizenship, and it is changeable at the user's discretion (though not without considerable inconvenience). Is control via limited exit options enough to redeem a lack of democratic rights?

Third, if companies hold themselves out as "Digital Switzerlands," capable of and indeed engaged in public functions, should they be held to the public-law values imposed on governments—values like accountability, transparency, due process, and the protection of privacy and security? If so, how?

Finally, the companies have shifted from colluding with to countering governments at least some of the time—and they could easily switch back. If there is value in the companies acting as Digital Switzerlands, how can this role be entrenched?

To be clear, this Article primarily addresses the companies' relationships to governments. It does *not* focus on the many significant issues surrounding technology companies' relationships with their users in general,[6] though as

6 These issues are myriad, including, for example, the companies' appropriate role in content moderation, the extent to which platforms are discriminatory, transparency to users about how the companies use and sell their data, the effect of social media on society, and whether the companies should be reined in by antitrust laws. *See, e.g.*, FOER, *supra* note 2, at 203-04 ("The health of our democracy demands that we consider treating Facebook, Google, and Amazon with the same firm hand that led government to wage war on AT&T, IBM, and Microsoft—even dismembering them into smaller companies if circumstances (and the law) demand a forceful response."); Anupam Chander & Vivek Krishnamurthy, *The Myth of Platform Neutrality*, 2 GEO. L. TECH. REV. 400, 413-15 (2018) (discussing conservative critiques of platforms as biased); Rahman, *supra* note 2, at 1669 (proposing regulating Internet platforms as public utilities in order to remedy problems like "outsized abilities to set the terms of exchange" and the ability to "exploit . . . the mountains of data" platforms collect that "can enable subtle forms of pricing, racial, and geographic discrimination"); Zeynep Tufekci,

the Conclusion highlights, the rise of Digital Switzerlands may have implications for company–user dynamics as well.[7]

This Article proceeds in three parts. Part I traces the parallel evolutions of governments' role vis-à-vis cyberspace and companies' role vis-à-vis governments and distinguishes the U.S. technology companies from potential historical and contemporary analogues. Part II unpacks the idea of "Digital Switzerland," exploring the accuracy of the embedded claims of parity and neutrality, and offering a model to describe when the Digital Switzerland mantle will lead the companies to challenge governments (or not). Part III identifies key criteria for normatively assessing the rise of technology companies as Digital Switzerlands and offers preliminary evaluations of the companies' performance to date.

I. THE PARALLEL EVOLUTION OF COMPETING POWERS

The roles of governments and technology companies vis-à-vis cyberspace have evolved along separate, but occasionally intersecting tracks, leaving U.S.

Opinion, *We Already Know How to Protect Ourselves from Facebook*, N.Y. TIMES (Apr. 9, 2018), https://www.nytimes.com/2018/04/09/opinion/zuckerberg-testify-congress.html (proposing to address data privacy and aggregation concerns through legislative action, for example, to give individuals access to data companies collect about them); Susan Landau, *No, Facebook, It's Not About Security; It's About Privacy*, LAWFARE (Mar. 26, 2018, 8:00 AM), https://www.lawfareblog.com/no-facebook-its-not-about-security-its-about-privacy [https://perma.cc/4U5M-KQ7H] (arguing that the Cambridge Analytica scandal is "a failure to protect the privacy of users' data" and that Facebook cannot adequately address the problem because "sharing of user data lies at the heart of Facebook's business"); Frank Pasquale, *From Territorial to Functional Sovereignty: The Case of Amazon*, LAW & POL. ECON. (Dec. 6, 2017), https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon [https://perma.cc/LY9W-B7WZ] (using a political economy perspective to express concern about the power of "major digital firms" that "are no longer market participants," but "market makers, able to exert regulatory control over the terms on which others can sell goods and services"); *see also infra* note 201 and accompanying text. These important issues deserve their own treatments, as others have undertaken, and the role of this Article is to address a different and distinct feature of the technology companies' behavior. That is not, however, to say that there is no overlap. For example, recent controversies over the use of Facebook to influence U.S. voters implicate both the relationship of the company to its users and the company's role in international struggles between governments. *See* Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, GUARDIAN (Mar. 17, 2018, 18:03 EDT), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [https://perma.cc/BZ6X-CMW2] (detailing how Cambridge Analytica used data gathered from Facebook to target U.S. voters); Tony Romm, *'Pro-Beyoncé' vs. 'Anti-Beyoncé': 3,500 Facebook Ads Show the Scale of Russian Manipulation*, WASH. POST (May 10, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/10/here-are-the-3400-facebook-ads-purchased-by-russias-online-trolls-during-the-2016-election [https://perma.cc/8TPZ-BRXW] (reporting on "Facebook ads purchased by Russian agents" that "illustrate the extent to which Kremlin-aligned forces sought to stoke social, cultural and political unrest on one of the Web's most powerful platforms").

7 *See infra* note 315 and accompanying text.

technology companies in a position somewhat different from the roles played by other powerful historical and contemporary private parties.

A. *Governments and Cyberspace*

The most obvious powers in cyberspace today are governments. Governments regulate behavior in cyberspace, impose taxes on Internet sales, exploit electronic communications for surveillance, and conduct offensive and defensive operations against other governments and malicious actors. But the possibility and legitimacy of these governmental roles was not always so obvious. Beginning in the 1990s, academic theorizing about the role of governments with respect to cyberspace has progressed through three stages.[8]

In the early days of the Internet, the first generation of activists and academics argued that cyberspace was outside the power of territorial governments and subject to rule only by its users.[9] David Johnson and David Post argued that "[c]yberspace . . . needs and can create its own law and legal institutions," separate and apart from existing territorial governments and their legal regimes.[10]

The cyber-as-sovereign arguments provoked an academic backlash and a practical defeat. The second generation of theorists argued that existing territorial governments could and should exercise sovereignty over cyberspace. Jack Goldsmith argued that territorial sovereignty's relationship to cyberspace is straightforward: governments can regulate "persons within the territory who use the Internet," hardware and software in the government's territory, and "the local effects of extraterritorial acts."[11] Normatively, Goldsmith and Tim Wu argued that government regulation is necessary and desirable because "only traditional territorial governments can provide [public] goods,"[12] and effectively deal with threats like "viruses, online fraud, spam, and other abuses."[13] As a practical matter, governments now regulate online behavior extensively, through criminal laws and other regulations. The traditional sovereigns—states—clearly and forcefully exert their power over individuals in cyberspace.

---

8 For a more detailed exposition of the three generations, see Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 325-29 (2015).

9 *See, e.g.*, David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) (arguing that the transborder nature of Internet-based communications "undermin[es] the feasibility—and legitimacy—of laws based on geographic boundaries"); John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence [https://perma.cc/YHM7-SZLX] ("Governments of the Industrial World . . . have no sovereignty where we gather.").

10 Johnson & Post, *supra* note 9, at 1367.

11 Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475, 476 (1998).

12 JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 142 (2006).

13 *Id.* at 145.

The third and most recent generation of academic work shifts from considering the role of territorial sovereigns vis-à-vis individuals, and instead focuses on issues of Internet governance and lawful state behavior in cyberspace.[14] This work is driven by recent contests between states over issues like competing visions of Internet governance[15] and by debates over whether and if so, how existing international law applies to states' actions in cyberspace.[16]

While commentators have paid considerable attention to the evolving role of governments, less attention has been paid to a parallel and ongoing evolution featuring technology companies.

B. *Technology Companies and Cyberspace*

In recent years, major U.S. technology companies have grown into power centers that compete with territorial governments.[17] They are now beginning to be, in some senses, competing sovereigns,[18] and self-consciously so.

---

14 *See, e.g.*, LAURA DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE 23 (2014) ("A significant question of Internet governance addresses the appropriate balance of power between sovereign nation-state governance and non-territorial and privatized mechanisms."); MILTON MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 9 (2010) ("*Internet governance* is the simplest, most direct, and inclusive label for the ongoing set of disputes and deliberations over how the Internet is coordinated, managed, and shaped to reflect policies."); Eichensehr, *supra* note 8 (discussing the development of norms for state behavior in cyberspace); Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 AM. J. INT'L L. 425, 427-29 (2016) (offering a process-oriented approach to construction of norms for appropriate state behavior in cyberspace); Kal Raustiala, Editorial Comment, *Governing the Internet*, 110 AM. J. INT'L L. 491, 492 (2016) (discussing the U.S. strategy with respect to Internet governance).

15 *See, e.g.*, Eichensehr, *supra* note 8, at 330-32 (discussing states' competing visions of multistakeholder and multilateral Internet governance); Raustiala, *supra* note 14, at 492 (arguing that U.S. relinquishment of control over ICANN will strengthen "multistakeholderism . . . not just for ICANN, but as a broader principle of global governance").

16 For example, Russia's hacking and interference in the 2016 U.S. elections has sparked debate about the scope of the prohibition on intervention. *See, e.g.*, Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579, 1580 (2017) (arguing that Russia's actions violated the right to self-determination); Ryan Goodman, *International Law and the US Response to Russian Election Interference*, JUST SEC. (Jan. 5, 2017), https://www.justsecurity.org/35999/international-law-response-russian-election-interference [https://perma.cc/D9T8-JR9N] (discussing international law regarding the Democratic National Committee (DNC) hack and the U.S. response thereto); Duncan Hollis, *Russia and the DNC Hack: What Future for a Duty of Non-Intervention*, OPINIO JURIS (July 25, 2016), http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention [https://perma.cc/A4C8-6CJ7] (discussing the scope of the international law prohibition on intervention).

17 The limitation to U.S. companies is a deliberate one. *See infra* note 79 and accompanying text.

18 *See, e.g.*, BERKMAN CTR. FOR INTERNET & SOC'Y AT HARVARD UNIV., DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE 9 (2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/BG3X-NNUQ] (noting that U.S. tech companies "are increasingly playing a quasi-sovereign role as they face difficult decisions when foreign government agencies pressure them to produce data about citizens abroad"); REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE

Facebook CEO Mark Zuckerberg has said, "In a lot of ways Facebook is more like a government than a traditional company."[19]

That was not always the case. Technology companies have a history of collaborating with, rather than challenging, both foreign governments and the United States.[20] In the early to mid-2000s, many of the U.S. technology companies entered the Chinese market. To do business in China, the companies faced demands from the Chinese government,[21] and some of their actions in response to such requests drew particular ire. Most infamously, Yahoo complied with Chinese government requests to turn over email records of two Chinese dissidents, who were then convicted and imprisoned.[22] In a February 2006 hearing, U.S. congressmen excoriated Cisco Systems, Google,

---

STRUGGLE FOR INTERNET FREEDOM 154 (2012) (arguing that U.S. tech companies "operate a kind of private sovereignty in cyberspace"); Anupam Chander, *Facebookistan*, 90 N.C. L. REV. 1807, 1808 (2012) ("Facebook has become so powerful and omnipresent that some have begun to employ the language of nationhood to describe it."); Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 199 (2017) ("Dominant platforms' role in the international legal order increasingly resembles that of sovereign states."); Sheera Frenkel et al., *Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis*, N.Y. TIMES (Nov. 14, 2018), https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html ("Facebook has connected more than 2.2 billion people, a global nation unto itself that reshaped political campaigns, the advertising business and daily life around the world."); Michael Joseph Gross, *Enter the Cyber-Dragon*, VANITY FAIR (Aug. 2, 2011, 12:00 AM), http://www.vanityfair.com/news/2011/09/chinese-hacking-201109 [https://perma.cc/M6Z4-7Y5B] ("You see Google acting in some ways as nation-states used to act, exercising to the best of their ability some attributes traditionally associated with sovereign states. We're going to break relationships—cease doing business there . . . ." (internal quotation marks omitted) (quoting former NSA Director Michael Hayden)). *But see* ANDREW KEANE WOODS, HOOVER INST., TECH FIRMS ARE NOT SOVEREIGNS 1 (2018), https://www.hoover.org/sites/default/files/research/docs/woods_webreadypdf.pdf [https://perma.cc/74JC-VAAX] (arguing that tech firms are not a serious threat to state sovereignty).

19 DAVID KIRKPATRICK, THE FACEBOOK EFFECT: THE INSIDE STORY OF THE COMPANY THAT IS CONNECTING THE WORLD 254 (2011).

20 *See, e.g.*, Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, VA. J.L. & TECH., Summer 2003, at 1, ¶¶ 2-3 (noting that private technology companies were "recruited, or co-opted, to serve the State" and that many "volunteer[ed] to join the State's efforts," citing eBay's policy on disclosures to law enforcement); Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COMM. REG. 595, 621 (2004) (detailing eBay's policy circa 2003 of turning information over to law enforcement absent a court order).

21 Prominent among the demands was censoring of search results. *See, e.g.*, Clive Thompson, *Google's China Problem (and China's Google Problem)*, N.Y. TIMES MAG. (Apr. 23, 2006), http://www.nytimes.com/2006/04/23/magazine/23google.html (describing Google's decision to enter the Chinese market in 2006 and the choices it made about how to censor search results).

22 *See, e.g.*, Joseph Kahn, *Yahoo Helped Chinese to Prosecute Journalist*, N.Y. TIMES (Sept. 8, 2005), http://www.nytimes.com/2005/09/08/business/worldbusiness/yahoo-helped-chinese-to-prosecute-journalist.html (detailing the case of Shi Tao, who was sentenced to a ten-year prison term); Elinor Mills, *Yahoo Settles Lawsuit with Jailed Chinese Journalists*, CNET (Nov. 13, 2007, 7:41 PM GMT), https://www.cnet.com/uk/news/yahoo-settles-lawsuit-with-jailed-chinese-journalists (reporting that Yahoo settled a case brought by Shi Tao and Wang Xiaoning, journalists serving prison sentences as a result of information that Yahoo disclosed to the Chinese government).

Microsoft, and Yahoo for what Representative Christopher Smith deemed "'sickening collaboration' with the Chinese government."[23] No doubt driven in part (perhaps large part) by negative publicity stemming from cooperation with the Chinese government,[24] those companies slowly began to shift to countering foreign governments on some fronts.[25]

1. Countering Foreign Governments

The first significant public move to challenge a foreign government came in January 2010.[26] In a blog post by Chief Legal Officer David Drummond, Google announced "[a] new approach to China."[27] The post explained that in December 2009, Google discovered a "highly sophisticated and targeted attack on [Google's] corporate infrastructure originating from China that resulted in the theft of intellectual property from Google."[28] But Google explained that it had "evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists" and that "the accounts of dozens of U.S., China and Europe based Gmail users who are advocates of human rights in China appear to have been routinely accessed by third parties."[29] While Google did not directly accuse the Chinese

---

23 Tom Zeller Jr., *Web Firms Are Grilled on Dealings in China*, N.Y. TIMES (Feb. 16, 2006), http://www.nytimes.com/2006/02/16/technology/web-firms-are-grilled-on-dealings-in-china.html.

24 *See, e.g.*, Marc Gunther, *Tech Execs Get Grilled over China Business*, FORTUNE (Feb. 16, 2006, 10:43 AM EST), http://money.cnn.com/2006/02/15/news/international/pluggedin_fortune [https://perma.cc/PU5H-4T7H] ("[T]he controversy has taken some of the glow off the image promoted by Internet firms like Yahoo and Google.").

25 *See infra* Section II.C (discussing the scope of the Digital Switzerlands idea, including when companies will challenge governments and the difficulties posed by nondemocratic governments).

26 Although this Article focuses on U.S. technology companies, the willingness to challenge governments is not a purely U.S. phenomenon. For example, Blackberry, a Canadian company, *see Company*, BLACKBERRY, https://ca.blackberry.com/company [https://perma.cc/A6SL-58F3] (last visited Feb. 8, 2019), announced that it would exit the Pakistani market rather than comply with the Pakistani government's demand to monitor communications made using Blackberry's network in the country. Marty Beard, *Why BlackBerry Is Exiting Pakistan*, BLACKBERRY: INSIDE BLACKBERRY (Nov. 30, 2015), http://blogs.blackberry.com/2015/11/why-blackberry-is-exiting-pakistan [https://perma.cc/8GQ6-M769]. Ultimately, the Pakistani government apparently backed down, and BlackBerry continued to operate in the country. *See* Marty Beard, *Continuing Our Operations in Pakistan*, BLACKBERRY: INSIDE BLACKBERRY (Dec. 31, 2015), http://blogs.blackberry.com/2015/12/continuing-our-operations-in-pakistan [https://perma.cc/HN7Y-QMKV] (explaining that BlackBerry is "grateful to the . . . Pakistani government for accepting BlackBerry's position that we cannot provide the content of our customers' BES traffic, nor will we provide access to our BES servers").

27 David Drummond, *A New Approach to China*, GOOGLE (Jan. 12, 2010), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html [https://perma.cc/C8PL-QHRS].

28 *Id.* The post further explained that "at least twenty other large companies . . . have been similarly targeted." *Id.*; *see also* SHANE HARRIS, @WAR: THE RISE OF THE MILITARY INTERNET COMPLEX 172 (2014) (noting other targets, including Adobe, Juniper Networks, Northrup Grumman, Symantec, and Yahoo).

29 Drummond, *supra* note 27.

government, it tied the revelations to "a much bigger global debate about freedom of speech," and explained: "These attacks and the surveillance they have uncovered—combined with the attempts over the past year to further limit free speech on the web—have led us to conclude that we should review the feasibility of our business operations in China."[30]

Google's post and the challenge it posed to the Chinese government marked a major milestone. At the time, the press called it a "highly unusual rebuke of China by one of the largest and most admired technology companies,"[31] and a "startling announcement."[32] In retrospect, the move has been called "historic."[33]

---

30 *Id.* Google announced that it would cease censoring search results, which it had done since entering the Chinese market. *Id.* In March 2010, Google stopped censoring search results on Google.cn and instead redirected users to uncensored searching on its website in Hong Kong. David Drummond, *A New Approach to China: An Update*, GOOGLE (Mar. 22, 2010), https://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html [https://perma.cc/PD5G-P85N]; *see* Ellen Nakashima, Cecelia Kang & John Pomfret, *Google to Stop Censoring Search Results in China*, WASH. POST (Mar. 23, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/03/22/AR2010032202041.html [https://perma.cc/748T-MBVT] (reporting Google's decision to redirect searches through Hong Kong). Several months later, as a condition of a license renewal that allowed Google to continue operating in China, Google ceased automatically redirecting users to the Hong Kong site, instead posting a link on Google.cn that allowed users to reach the Hong Kong site, while using Google.cn for music and other searches that remained unfiltered. *See* David Drummond, *An Update on China*, GOOGLE (June 28, 2010), https://googleblog.blogspot.com/2010/06/update-on-china.html [https://perma.cc/Z8B5-88XK] (last updated July 9, 2010) (noting that China renewed Google's license to operate); *Google Says China License Renewed by Government*, BBC (July 9, 2010), http://www.bbc.com/news/10566318 [https://perma.cc/YL99-YGRZ] (describing Google's actions to secure the license renewal).

31 Andrew Jacobs & Miguel Helft, *Google, Citing Attack, Threatens to Exit China*, N.Y. TIMES (Jan. 12, 2010), http://www.nytimes.com/2010/01/13/world/asia/13beijing.html.

32 Kim Zetter, *Google to Stop Censoring Search Results in China After Hack Attack*, WIRED (Jan. 12, 2010, 7:10 PM), https://www.wired.com/2010/01/google-censorship-china [https://perma.cc/5TLM-DWZX].

33 *See* HARRIS, *supra* note 28, at 173 ("For any company to come out against China would be momentous. But for Google, the most influential company of the Internet age, it was historic."); *see also* Sarah McKune & Ronald Deibert, *Google's Dragonfly: A Bellweather for Human Rights in the Digital Age*, JUST SEC. (Aug. 2, 2018), https://www.justsecurity.org/59941/googles-dragonfly-bellwether-human-rights-digital-age [https://perma.cc/YKS6-WBSQ] (calling Google's exit "a bold, nearly unheard of action by a corporate actor in the face of pressure by one of the world's most powerful governments"). Recent reports suggest that Google is considering re-entering the Chinese market with a mobile search engine that will censor results. Ryan Gallagher, *Google Plans to Launch Censored Search Engine in China, Leaked Documents Reveal*, INTERCEPT (Aug. 1, 2018, 4:58 AM), https://theintercept.com/2018/08/01/google-china-search-engine-censorship [https://perma.cc/3YL2-ZBV4]. The reports have prompted privacy-based criticism. *See, e.g.*, Michael C. Bender & Dustin Volz, *Pence Calls on Google to Drop Mobile Search Project in China*, WALL ST. J. (Oct. 4, 2018, 5:10 PM ET), https://www.wsj.com/articles/pence-calls-on-google-to-drop-mobile-search-project-in-china-1538680844 (reporting a speech in which U.S. Vice President Mike Pence urged Google to "immediately end development of the Dragonfly app that will strengthen Communist Party censorship and compromise the privacy of Chinese customers"); Kate Conger, *Ex-Google Employee Urges Lawmakers to Take on Company*, N.Y. TIMES (Sept. 26, 2018), https://www.nytimes.com/2018/09/26/technology/google-privacy-china-congress.html (discussing a letter from a former Google employee to senators criticizing "Dragonfly," the Chinese search engine product, on privacy grounds). Criticisms, including by Google employees, appear to have halted the project for now. *See* Aaron Mak, *Hundreds of Employees Demand Google Stop Work on Censored*

Google pioneered another means of countering foreign governments. In June 2012, the company announced that it would begin warning users who the company believed were being targeted by foreign governments.[34] The warning is delivered by a banner at the top of a Google login page, stating "Warning: We believe state-sponsored attackers may be attempting to compromise your account or computer," and linking users to advice on how to protect the security of their accounts.[35] In 2015, other companies followed Google's lead.[36] Facebook,[37] Yahoo,[38] and Microsoft[39] all announced that they will notify users that the companies believe are being targeted by state-sponsored actors.[40] The companies combine the warnings with instructions on how to re-secure or better secure the users' accounts, thus thwarting the attacks by the state-sponsored hackers.[41]

Search Engine for China, SLATE (Nov. 27, 2018, 4:47 PM), https://slate.com/technology/2018/11/google-employees-sign-petition-to-end-project-dragonfly.html [https://perma.cc/F6TX-ANTJ] (discussing open letter signed by hundreds of Google employees); *see also* Ryan Gallagher, *Google's Secret China Project "Effectively Ended" After Internal Confrontation*, INTERCEPT (Dec. 17, 2018, 12:22 PM), https://theintercept.com/2018/12/17/google-china-censored-search-engine-2 (reporting that progress on Dragonfly has halted).

34 Eric Grosse, *Security Warnings for Suspected State-Sponsored Attacks*, GOOGLE: SEC. BLOG (June 5, 2012), https://security.googleblog.com/2012/06/security-warnings-for-suspected-state.html [https://perma.cc/ER7P-D3SH].

35 *Id.* (emphasis omitted).

36 *See* Kristen Eichensehr, *"Your Account May Have Been Targeted by State-Sponsored Actors": Attribution and Evidence of State-Sponsored Cyberattacks*, JUST SEC. (Jan. 11, 2016), https://www.justsecurity.org/28731/your-account-targeted-state-sponsored-actors-attribution-evidence-state-sponsored-cyberattacks [https://perma.cc/5BLN-2S47] (collecting and analyzing the companies' announcements).

37 Alex Stamos, *Notifications for Targeted Attacks*, FACEBOOK (Oct. 16, 2015, 7:36 PM), https://www.facebook.com/notes/facebook-security/notifications-for-targeted-attacks/10153092994615766 [https://perma.cc/8UJP-SKJR]. Facebook's notification system reportedly provided the first indication that Iranian hackers compromised the accounts of State Department officials working on Iran and the Middle East. David E. Sanger & Nicole Perlroth, *Iranian Hackers Attack State Dept. via Social Media Accounts*, N.Y. TIMES (Nov. 24, 2015), https://www.nytimes.com/2015/11/25/world/middleeast/iran-hackers-cyberespionage-state-department-social-media.html.

38 Bob Lord, *Notifying Our Users of Attacks by Suspected State-Sponsored Actors*, YAHOO SEC. (Dec. 21, 2015), https://yahoo-security.tumblr.com/post/135674131435/notifying-our-users-of-attacks-by-suspected [https://perma.cc/F4AS-EBM7].

39 Scott Charney, *Additional Steps to Help Keep Your Personal Information Secure*, MICROSOFT: MICROSOFT ON THE ISSUES (Dec. 30, 2015), https://blogs.microsoft.com/on-the-issues/2015/12/30/additional-steps-to-help-keep-your-personal-information-secure [https://perma.cc/6GZ9-Z7VX].

40 Although it did not announce a formal policy, Twitter similarly began notifying users targeted by state-sponsored actors. *See, e.g.*, Ashley Carman, *Twitter Users Targeted by State-Sponsored Attackers*, VERGE (Dec. 12, 2015, 9:32 AM EST), https://www.theverge.com/2015/12/12/9931178/twitter-state-sponsored-attack [https://perma.cc/6PJH-6NSX] (reporting that some Twitter users received notifications stating that their accounts "may have been targeted by state-sponsored actors" (quoting @Anne_Roth, TWITTER (Dec. 11, 2015, 8:11 PM), https://twitter.com/Anne_Roth/status/675467882407591936 [https://perma.cc/8VGE-V7G3])).

41 *See* Charney, *supra* note 39; Grosse, *supra* note 34; Lord, *supra* note 38; Stamos, *supra* note 37.

2. Countering All Governments—Sometimes

U.S. technology companies' moves to counter governments accelerated with the Snowden disclosures and refocused on countering the U.S. government. The Snowden disclosures began in June 2013 and fundamentally changed the calculus regarding cooperation with the U.S. government.[42] While companies had previously assisted the government, even above and beyond their legal obligations to do so,[43] as a result of disclosures, "[t]here is now business value in championing privacy and fighting" the U.S. government "and business harm in cooperation."[44]

The companies' shift to a more adversarial stance toward the U.S. government occurred quickly. One of the early reports based on documents leaked by Edward Snowden in June 2013 indicated that pursuant to a program called "PRISM," "[t]he National Security Agency and the FBI [were] tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, emails, documents, and connection logs."[45] The report indicated that the government collected information directly from servers owned by Apple, Facebook, Google, Microsoft, and Yahoo, among others, prompting the companies to vehemently deny that they permitted such access.[46] Days later, after "intense talks between federal officials and several of the technology companies . . . over what details [could] be released" about government information requests,[47] Google filed a motion for a declaratory judgment with the Foreign Intelligence Surveillance Court, arguing for a First Amendment right to publish aggregate information on the number of Foreign Intelligence Surveillance Act (FISA) orders it

---

42 *See* DAVID E. SANGER, THE PERFECT WEAPON: WAR, SABOTAGE, AND FEAR IN THE CYBER AGE 85 (2018) ("The Snowden affair kicked off a remarkable era in which American firms, for the first time in post–World War II history, broadly refused to cooperate with the American government.").

43 *See* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 910-16 (2008) (providing details of assistance that U.S. telecommunications and other companies voluntarily provided to the U.S. government after the September 11 attacks); *see also supra* note 20 and accompanying text.

44 BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 207 (2015); *see also* ADAM SEGAL, THE HACKED WORLD ORDER: HOW NATIONS FIGHT, TRADE, MANEUVER, AND MANIPULATE IN THE DIGITAL AGE 20 (2016) ("American companies are now more willing to stand up to Washington and to align with the interests of global customers.").

45 Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), 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 [https://perma.cc/EP5F-BU9A].

46 *Id.*

47 Craig Timberg & Cecilia Kang, *Google Challenges U.S. Gag Order, Citing First Amendment*, WASH. POST (June 18, 2013), https://www.washingtonpost.com/business/technology/google-challenges-us-gag-order-citing-first-amendment/2013/06/18/96835c72-d832-11e2-a9f2-42ee3912ae0e_story.html [https://perma.cc/PAT3-MXSL].

receives and the number of users covered by the requests.[48] The lawsuit "[came] as the firms increasingly show[ed] signs of wanting to outdo each other in demonstrating their commitment to protecting user privacy."[49] Ultimately, Facebook, Microsoft, Yahoo, and LinkedIn also challenged the gag rules, and the confrontation ended in January 2014 with a compromise allowing the companies to disclose additional information about government requests for customer data pursuant to national security letters and FISA orders.[50]

Additional litigation to resist U.S. government demands and gag orders has followed. A prominent example was the dispute between the U.S. government and Apple over access to the iPhone of one of the San Bernardino shooters. The Department of Justice obtained an order from a magistrate judge to compel Apple to write code that would have disabled some of the phone's security features, including by allowing the government an unlimited number of attempts to guess the phone's passcode.[51] Apple resisted the order in court[52] and in the court of public opinion.[53] On the eve of a hearing, the government ultimately dropped its demand for Apple's assistance, revealing that it had paid a private party for a tool to access the iPhone.[54]

---

48 *See Google's Motion for Declaratory Judgment*, WASH. POST (June 18, 2013), http://apps.washingtonpost.com/g/page/business/googles-motion-for-declaratory-judgment/238 [https://perma.cc/7JCF-RXFE] (providing text of *In re Motion for Declaratory Judgment of Google Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders*, as filed with the Foreign Intelligence Surveillance Court).

49 Timberg & Kang, *supra* note 47.

50 *See* Letter from James M. Cole, Deputy Attorney Gen., U.S. Dep't of Justice, to Colin Stretch, Vice President & Gen. Counsel, Facebook, et al. (Jan. 27, 2014), https://www.justice.gov/iso/opa/resources/366201412716018407143.pdf [https://perma.cc/TJ36-42Q9]) (detailing what information companies may release and when); *see also* Matt Apuzzo & Nicole Perlroth, *U.S. Relaxes Some Data Disclosure Rules*, N.Y. TIMES (Jan. 27, 2014), https://www.nytimes.com/2014/01/28/business/government-to-allow-technology-companies-to-disclose-more-data-on-surveillance-requests.html (describing new rules for disclosure).

51 Order Compelling Apple, Inc. to Assist Agents in Search at 2, *In re* the Search of an Apple Iphone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451 (C.D. Cal. Feb. 16, 2016), 2016 WL 618401, at *1.

52 Apple, Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, & Opposition to Government's Motion to Compel Apple's Assistance, *In re* the Search of an Apple Iphone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. CM 16-10 (C.D. Cal. Feb. 25, 2016) [hereinafter Apple, Inc.'s Motion to Vacate Order].

53 *See* Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter [https://perma.cc/S4UF-B8J4] ("Opposing this order is not something we take lightly. We feel we must speak up in the face of what we see as an overreach by the U.S. government.").

54 Government's *Ex Parte* Application for a Continuance at 3, *In re* the Search of an Apple Iphone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. CM 16-10 (C.D. Cal. Mar. 21, 2016); Eric Lichtblau & Katie Benner, *F.B.I. Director Suggests Bill for iPhone Hacking Topped $1.3 Million*, N.Y. TIMES (Apr. 21, 2016), http://www.nytimes.com/2016/04/22/us/politics/fbi-director-suggests-bill-for-iphone-hacking-was-1-3-million.html; *see also* LUCAS KELLO, THE VIRTUAL WEAPON AND INTERNATIONAL ORDER 182 (2017) (arguing that this episode shows that "the private sector was supreme over the sovereign" because "the world's most powerful government overcame the resistance of company executives more powerful than itself in dealing

Microsoft has also brought several suits. In one recent case, Microsoft resisted complying with a warrant issued pursuant to the Stored Communications Act for the contents of an email account stored in Ireland.[55] Microsoft provided the government with the noncontent account information stored in the United States, but argued that, as to the content stored in Ireland, the warrant was an impermissible exercise of extraterritorial jurisdiction.[56] The Second Circuit agreed with Microsoft,[57] and the Supreme Court granted review.[58] Congress passed a bill mooting the case before the Supreme Court could resolve it.[59]

In another case, Microsoft sued the Department of Justice, arguing that a provision of the Electronic Communications Privacy Act (ECPA) is unconstitutional.[60] In particular, the company argued that the ECPA provision allowing courts to impose gag orders that prevent the company from alerting customers when the government seeks access to the customers' email or other information violates the First and Fourth Amendments.[61] Microsoft prevailed. The Department of Justice issued a new binding policy, limiting the use and duration of secrecy orders,[62] and Microsoft, declaring the policy an "unequivocal win for [its] customers," moved to dismiss the lawsuit.[63]

These steps by U.S. technology companies to challenge foreign governments and the U.S. government focus mostly on the negative—countering government action. What was missing was an affirmative theory to describe the role the companies are playing. That began to change in 2017.

---

with a matter of national security significance only because the state recruited or bought the sympathies of another private player").

55 Microsoft Corp. v. United States, 829 F.3d 197, 200 (2d Cir. 2016), *reh'g en banc denied*, 855 F.3d 53 (2d Cir. 2017), *cert. granted*, 138 S. Ct. 356 (2017). For additional analysis of the Microsoft case and extraterritorial jurisdiction issues, see Kristen E. Eichensehr, *Data Extraterritoriality*, 95 TEX. L. REV. *SEE ALSO* 145, 149-53 (2017).

56 Eichensehr, *supra* note 55, at 149-50.

57 *Id.* at 150.

58 United States v. Microsoft Corp., 138 S. Ct. 356 (2017).

59 *See* United States v. Microsoft Corp., 138 S. Ct. 1186, 1187-88 (2018) (acknowledging that the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) rendered the case moot, and vacating and remanding with instructions to dismiss as moot).

60 Complaint for Declaratory Judgment at 1-4, Microsoft Corp. v. U.S. Dep't of Justice, No. 2:16-cv-00538 (W.D. Wash. Apr. 14, 2016); *see Developments in the Law—More Data, More Problems*, 131 HARV. L. REV. 1714, 1738 (2018) (calling this lawsuit "an example of surveillance intermediaries at their best" because "Microsoft noticed a pattern of the government overusing secrecy orders and mobilized its considerable resources to change this practice . . . [doing] so of its own volition").

61 Complaint for Declaratory Judgment, *supra* note 60, at 9-16.

62 Nick Wingfield, *U.S. to Limit Use of Secrecy Orders That Microsoft Challenged*, N.Y. TIMES (Oct. 24, 2017), https://www.nytimes.com/2017/10/24/business/microsoft-justice-department-secrecy.html.

63 Brad Smith, *DOJ Acts to Curb the Overuse of Secrecy Orders. Now It's Congress' Turn*, MICROSOFT: MICROSOFT ON THE ISSUES (Oct. 23, 2017), https://blogs.microsoft.com/on-the-issues/2017/10/23/doj-acts-curb-overuse-secrecy-orders-now-congress-turn [https://perma.cc/5NPN-RUBE].

3. An Emerging Affirmative Platform?

In a keynote speech at the 2017 RSA conference, Microsoft President Brad Smith provided a new, positive label for the role of technology companies in the cyberspace ecosystem.[64] Smith called for the "global technology sector . . . to become a trusted and neutral Digital Switzerland."[65] Smith exhorted technology companies to work together and argued:

> We need to be clear that we will assist and protect customers everywhere. That is what we do regardless of the country from which we come.
>
> We need to be clear that we will not aid in attacking customers anywhere, regardless of the government that may ask us to do so.[66]

The "Digital Switzerland" label shifts from the prior baseline of companies defining their role in opposition to governments to a potential and perhaps partial embrace of an affirmative platform going forward.[67] The phrase describes, however, an emerging posture that is still in its infancy and fraught with growing pains, as explored in detail in Part II.[68]

---

64 Smith, *supra* note 1, at 12. Smith's speech was not the first time that Microsoft officials had floated the Switzerland analogy. In remarks at New York University School of Law in April 2016, Microsoft Corporate Vice President Scott Charney also characterized the company as akin to Switzerland. *See* N.Y.U. Sch. of Law Ctr. on Law & Sec., *Governing Intelligence: Panel II: The New Transnational Oversight*, YOUTUBE (Apr. 21, 2016, 17:40), https://www.youtube.com/watch?v=3kTYMz-GSxA [https://perma.cc/85Q9-LBBH] [hereinafter *Governing Intelligence*] (statement of Scott Charney, Corporate Vice President, Microsoft Corp.) ("[W]hen one country attacks another country, whether it be an espionage program or a cyber military operation, for us, that's one customer attacking another customer. And either customer might ask us for support and help. And that's why . . . we have to . . . be Switzerland. We have to do defense and not offense.").

65 Smith, *supra* note 1, at 12.

66 *Id.* at 13; *see also id.* at 12 ("We need to be a global industry that the world can rely on to play 100 percent defense and zero percent offense.").

67 David Post has argued that Smith's Digital Switzerland speech embraces the view that he, David Johnson, and to some extent John Perry Barlow, advanced in the 1990s of cyberspace as a separate place, apart from the rule of territorial governments. David Post, *Microsoft's Brad Smith on Cyberattacks, Cybersecurity, and 'Cyberspace'*, WASH. POST (Mar. 10, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/03/10/microsofts-brad-smith-on-cyberattacks-cybersecurity-and-cyberspace [https://perma.cc/LN4W-A7PT]; *see supra* notes 9–10 and accompanying text. But according to Smith, it is the companies—the technology sector—that should be a Digital Switzerland; Smith does not argue, as Post suggests, that cyberspace *itself* is a place that should be akin to a neutral country. *See* Smith, *supra* note 1, at 12 ("[W]e as a global technology sector need to become a trusted and neutral Digital Switzerland."); *cf.* Milton Mueller, *Searching for that "Neutral Digital Switzerland"*, INTERNET GOVERNANCE PROJECT (Mar. 3, 2017), https://www.internetgovernance.org/2017/03/03/searching-for-that-neutral-digital-switzerland [https://perma.cc/ZHA8-9UAS] ("[T]he fact that Microsoft's President was willing to issue a 2017 version of the declaration of the independence of cyberspace is heartening.").

68 *See infra* notes 221–25 and accompanying text.

C. *Distinguishing Other Powerful Private Parties*

U.S. technology companies are by no means the first superempowered private parties.[69] Think of the British East India Company, which ruled India as a government despite its corporate form,[70] or recent examples like ExxonMobil. But three features of the U.S. technology companies, if taken together, suggest that they differ from other powerful private actors in ways that may facilitate their ability to serve as "Digital Switzerlands."[71]

1. *They aspire to be global, not national.*[72] The Digital Switzerlands concept depends on the companies' ability to remain, and be perceived as remaining, independent from governments, including their national government.[73] They

---

69 *Cf. The Rise of the Superstars*, ECONOMIST (Sept. 17, 2016), http://www.economist.com/news/special-report/21707048-small-group-giant-companiessome-old-some-neware-once-again-dominating-global?fsrc=scn/fb/te/pe/ed/theriseofthesuperstars [https://perma.cc/E7AP-PRP3] ("Apple, Google, Amazon and their peers dominate today's economy just as surely as US Steel, Standard Oil and Sears, Roebuck and Company dominated the economy of Roosevelt's day.").

70 Adam Smith referred to the situation as a "strange absurdity." ADAM SMITH, THE WEALTH OF NATIONS 602 (Edwin Cannan ed., Random House, Inc. 1937) (1776); *see* PHILIP J. STERN, THE COMPANY STATE: CORPORATE SOVEREIGNTY AND THE EARLY MODERN FOUNDATIONS OF THE BRITISH EMPIRE IN INDIA 3-6 (2012) (explaining that the British East India Company "did what early modern governments did," including "erect and administer laws; collect taxes, provide protection; inflict punishment; . . . conduct diplomacy and wage war"); ADAM WINKLER, WE THE CORPORATIONS: HOW AMERICAN BUSINESSES WON THEIR CIVIL RIGHTS 26 (2018) (noting with respect to the East India Company in the mid-1700s, that "[t]he corporation had become a government, with all the power that entails").

71 In addition to the differences discussed here, *The Economist* highlights another distinguishing feature of the technology companies as compared to earlier powerful corporations, namely that they have "few assets" and employees. *See The Rise of the Superstars*, *supra* note 69, at 5 (noting that with similar revenues, the top three U.S. carmakers in 1990 had 1.2 million employees, while the "top three companies in Silicon Valley" in 2014 had "just 137,000 employees").

72 They are also global, not (just) local. There are many precedents for private parties exercising extensive but *localized* control. Consider company towns where "a single business built, owned, and operated the entire town," often populated by the business's employees. M. Todd Henderson, *The Nanny Corporation*, 76 U. CHI. L. REV. 1517, 1535 (2009); *see* HARDY GREEN, THE COMPANY TOWN: THE INDUSTRIAL EDENS AND SATANIC MILLS THAT SHAPED THE AMERICAN ECONOMY 4-5 (2010) (contrasting "exploitationville" versus utopian company towns); Leanna Garfield, *Facebook and Amazon Are So Big They're Creating Their Own Company Towns—Here's the 200-Year Evolution*, BUS. INSIDER (Mar. 26, 2018, 9:27 AM), http://www.businessinsider.com/company-town-history-facebook-2017-9 [https://perma.cc/2853-MSR3] (discussing historical examples). Or cities like Detroit, where the car industry has dominated the area, despite not running an actual company town. Some of the tech companies are effectively creating company towns in parts of Silicon Valley. *See id*. (discussing Facebook in Menlo Park and Amazon in Seattle); Jessica Guynn, *Welcome to Zucker Burg*, L.A. TIMES (Aug. 10, 2012), http://articles.latimes.com/2012/aug/10/business/la-fi-facebook-company-town-20120810 [https://perma.cc/WBZ7-ZB8A] (discussing Facebook's construction of an extensive campus in Menlo Park). But the companies exercise different kinds of important powers over their users worldwide, and it is those powers—the global powers—that are the focus of this Article. *See infra* Part III.

73 *See* Mueller, *supra* note 67 ("Smith seems genuinely interested in detaching his company from national allegiances in favor of customer allegiance.").

therefore stand in stark contrast to companies, like Royal Dutch Shell or British Petroleum (BP), that embraced a national origin story,[74] and to prototypical government contractors, like Lockheed Martin or Northrop Grumman. As David Sanger recently highlighted, the companies have "a concept of corporate identity that is the complete reverse of the Cold War," where defense contractors "were serving governments, not consumers, and so . . . willingly picked a side."[75] By contrast, the tech companies "view themselves . . . as essentially neutral—loyal to the customer base first and individual governments second."[76]

The U.S. tech companies are also distinguishable from companies that are partly government-owned or controlled. This sets U.S. technology companies apart not only from older companies, like Volkswagen,[77] but also from technology companies headquartered in other parts of the world. For example, China has pushed for an ownership stake in and direct control over some of its biggest technology companies, including Tencent and Weibo.[78] It would be implausible for companies that are directly owned or controlled by governments—or under the threat of such ownership or control—to claim the mantles of neutrality and parity embedded in the Digital Switzerlands concept. Although all governments may regulate companies in their jurisdiction, the exertion of direct ownership or control is qualitatively different.

Today, the Digital Switzerlands concept is most likely limited to companies in the United States and Western Europe, where private companies are likely, though not certain, to remain independent of direct government control.[79] Companies in

---

74 Another contrast can be drawn between the consumer-focused technology companies and cybersecurity-specific companies. Companies, like FireEye from the United States and Kaspersky Labs from Russia, have been accused of differentially revealing cyber operations, specifically declining to reveal operations conducted by their own national government. *See* Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 492-93 (2017) (discussing allegations against cybersecurity companies of "pulling punches for national governments"). FireEye officials admitted in a recent interview that while they remove U.S. and allied intruders from their customers' systems, they refrain from publicizing such intrusions. Zaid Shoorbajee, *Playing Nice? FireEye CEO Says U.S. Malware Is More Restrained than Adversaries'*, CYBERSCOOP (June 1, 2018), https://www.cyberscoop.com/kevin-mandia-fireeye-u-s-malware-nice [https://perma.cc/W2SE-SMUL].

75 SANGER, *supra* note 42, at 267.

76 *Id*.

77 *See, e.g.*, Alison Smale, *In Germany, a Cozy Relationship Between Carmakers and Government*, N.Y. TIMES (Oct. 1, 2015), https://www.nytimes.com/2015/10/02/world/europe/germany-volkswagen-autos-merkel.html (noting that Volkswagen is partly owned by the government of Lower Saxony and that the regional governor holds a seat on the company's board).

78 Li Yuan, *Beijing Pushes for a Direct Hand in China's Tech Firms*, WALL ST. J. (Oct. 11, 2017, 7:27 PM ET), https://www.wsj.com/articles/beijing-pushes-for-a-direct-hand-in-chinas-big-tech-firms-1507758314.

79 For example, the signatories to the Cybersecurity Tech Accord, *see infra* notes 132–35 and accompanying text, come from the United States, Finland, and Spain, and do not include companies from countries identified as responsible for some of the major recent cyberattacks—countries like China, Iran, North Korea, and Russia. David E. Sanger, *Tech Firms Sign 'Digital Geneva Accord' Not to Aid Governments in Cyberwar*, N.Y. TIMES (Apr. 17, 2018), https://www.nytimes.com/2018/04/17/us/politics/tech-companies-cybersecurity-accord.html.

the United States and Western Europe that assert independence and challenge their governments run the risk of regulation, but not of nationalization.

2. *They have global users, not just customers or shareholders.* For some of the companies, their users are not customers in the traditional sense. Users of Facebook and Google do not pay money for the privilege.[80] For companies like Microsoft and Apple, the relationship may be partly transactional, but it also stretches into a long-term ongoing dependence, where users rely on the company for services and trust the company to keep potentially sensitive information secure.

The nature of the relationship between the technology companies and users therefore differs from a traditional transaction-focused relationship between companies and customers.[81] Unlike companies that merely sell goods to customers, the tech companies' relationship to their users is more intimate, more expansive, and more constant than even a series of recurring transactions.

3. *They are attractive, not extractive.* Powerful private companies, especially in earlier eras, were often headquartered in Europe or the United States and focused on extracting natural resources abroad. To do so they entered into agreements with foreign governments, setting the terms of their business's operations in the country. This system created little need for the companies to develop broad appeal among the populace in the countries where they operated, and in egregious instances, the companies committed or facilitated human rights violations against local populations.[82]

Some argue that certain tech companies—primarily those that derive revenue from using user data for ad sales[83]—are in fact extractive because of

---

80 *See infra* notes 84–89 and accompanying text.

81 *Cf.* JON D. MICHAELS, HOOVER INST., TECH GIANTS AT THE CROSSROADS: A MODEST PROPOSAL 3-4 (2018), https://www.hoover.org/sites/default/files/research/docs/michaels_webreadypdf.pdf [https://perma.cc/SR9F-84EE] (arguing that among the features that "distinguish[] the tech space" is that the "platforms at issue are ones that impinge on users' political rights and interests (making these firms different from, say, Walmart or General Motors)"); SEGAL, *supra* note 44, at 20-21 ("GM, Procter & Gamble (P&G), and Coca-Cola are global companies, but their relationships with their customers are relatively limited and transactional. They market and sell a product. . . . The technology companies' missions have been much more expansive . . . and so these companies have a more complicated, intense personal relationship to their customers that, if they have their way, will extend over years and into almost every aspect of users' lives."); Chander, *supra* note 18, at 1810 (distinguishing tech companies from earlier companies that "turn[ed] to the world as a market for goods," such as cars).

82 This is not to suggest that the technology companies are paragons of human rights virtues. *See, e.g.*, Charles Duhigg & David Barboza, *In China, Human Costs Are Built into an iPad*, N.Y. TIMES (Jan. 25, 2012), http://www.nytimes.com/2012/01/26/business/ieconomy-apples-ipad-and-the-human-costs-for-workers-in-china.html (detailing labor and safety issues in facilities that produce Apple products in China).

83 Not all tech companies profit from user data in this way. That is not Apple's business model, for example, and Apple's lack of dependence on user data has positioned it to criticize companies like Facebook and Google for their use of user data to sell advertising. *See, e.g.*, Natalia Drozdiak & Stephanie Bodoni, *'This Is Surveillance.' Apple CEO Tim Cook Slams Tech Rivals over Data Collection*, TIME (Oct. 24, 2018), http://time.com/5433499/tim-cook-apple-data-privacy [https://perma.cc/7XQD-UPEL] (reporting on Cook's comments at an European Union conference); *see also* JACK M. BALKIN, HOOVER INST., FIXING SOCIAL MEDIA'S GRAND BARGAIN 4 (2018), https://www.hoover.org/

the ways in which they profit from data collected from their users.[84] These critics discount the value of the "free" services provided in exchange for access to user information.[85] Recent academic proposals have even suggested that tech companies should pay users for the data they produce and from which the companies then derive benefit.[86]

However, the tech companies' relationship to user data is not extractive in the same way as earlier extractive enterprises. This produces a different power dynamic: whereas powerful companies in earlier eras sometimes resorted to hard power vis-à-vis local populations,[87] the technology companies operate through soft power.[88] Fundamentally, they depend on mass appeal to businesses, nongovernmental organizations, academic institutions, and individuals—their users. And these users are not captive audiences.[89] The

sites/default/files/research/docs/balkin_webreadypdf.pdf [https://perma.cc/93FQ-5B4P] ("The problem with the current business models for social media companies such as Facebook, Twitter, and YouTube is that they give companies perverse incentives to manipulate end users—or to allow third parties to manipulate end users—if this might increase advertising revenues, profits, or both."). Facebook and Google have responded by highlighting, among other points, the accessibility of their products to broader swaths of society because their products don't have a monetary price tag. *See* Drozdiak & Bodoni, *supra* (describing Facebook and Google's responses to Cook's critique).

84 *See* Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 79 (2015) (criticizing tech companies as extractive and arguing that "the methods of production of 'big data' from small data and the ways in which 'big data' are valued reflect the formal indifference that characterizes the firm's relationship to its populations of 'users'" and that "[p]opulations are the sources from which data extraction proceeds and the ultimate targets of the utilities such data produce").

85 *See id.* at 83 ("Google's tools are not the objects of a value exchange. They do not establish constructive producer-consumer reciprocities. Instead they are the 'hooks' that lure users into extractive operations and turn ordinary life into the daily renewal of a 21st-century Faustian pact.").

86 *See, e.g.*, Imanol Arrieta Ibarra et al., *Should We Treat Data as Labor? Moving Beyond "Free"*, 1 AM. ECON. ASS'N PAPERS & PROC. 1-5 (2018) (discussing a market for data as labor, rather than the current model of data as capital, pursuant to which technology companies would compensate data producers); Eduardo Porter, *Your Data Is Crucial to a Robotic Age. Shouldn't You Be Paid for It?*, N.Y. TIMES (Mar. 6, 2018), https://www.nytimes.com/2018/03/06/business/economy/user-data-pay.html (discussing arguments in favor of paying users for data, including increasing the quality of data provided).

87 ROBERT O. KEOHANE & JOSEPH S. NYE, POWER AND INTERDEPENDENCE 220 (3d ed. 2001) ("Hard power is the ability to get others to do what they otherwise would not do through threat of punishment or promise of reward. Whether by economic carrots or military sticks, the ability to coax or coerce has long been the central element of power.")

88 *See id.* ("Soft power . . . is the ability to get desired outcomes because others want what you want; it is the ability to achieve desired outcomes through attraction rather than coercion."); *see also* JOSEPH S. NYE, JR., THE FUTURE OF POWER 83 (2011) (noting that nongovernmental actors, including corporations, can wield soft power).

89 *See* Cohen, *supra* note 18, at 145 (noting that for platforms to succeed in "extracting the surplus value of user data . . . requires large numbers of users generating large amounts of data," and therefore "the platform provider's goal is to become and remain the indispensable point of intermediation for parties in its target markets" (footnote omitted)).

companies' success rests on a bottom-up strategy dependent on the continuing attractiveness and appeal of their products around the world.[90]

II. TECHNOLOGY COMPANIES AS DIGITAL SWITZERLANDS

The "Digital Switzerland" moniker captures two substantive ideas.[91] First, labeling technology companies as "Digital Switzerland" suggests that the companies are on par with the governments that try to regulate them. Second, the specific choice of Switzerland as the comparator suggests that the technology companies are not just countries, but *neutral* countries.[92] The following Sections analyze the extent to which the companies conform to these two premises and suggest a model for understanding their behavior consistent with the Digital Switzerlands idea.

A. *Parity*

The primacy that the Westphalian system places on the role of states makes the idea that companies are or should be on par with countries potentially revolutionary. Companies themselves have made some claims to parity,[93] but frequently it is academic and other commentators who compare the companies to countries.[94] In at least some ways, the claim may be descriptively plausible,[95] though the companies still fall short of state status in key ways.

Global Constituencies. Consider the companies' global constituencies. The user bases of the big U.S. technology companies dwarf the populations of the

---

90 *See* NYE, *supra* note 88, at 84 ("With soft power, what the target thinks is particularly important, and the targets matter as much as the agents . . . . Soft power is a dance that requires partners.").

91 The invocation of Switzerland may also bring to mind secrecy and privacy, given the country's long history of banking secrecy. But it's very unlikely that the tech companies intend to associate themselves with Switzerland's checkered history of banking secrecy, which includes tax evasion and resistance to returning Holocaust victims' accounts to their heirs. *See, e.g.*, Lynnley Browning, *A Swiss Bank Is Set to Open Its Secret Files*, N.Y. TIMES (Feb. 18, 2009), https://www.nytimes.com/2009/02/19/business/worldbusiness/19ubs.html (discussing U.S. Justice Department's settlement with UBS regarding tax evasion); Henry Weinstein, *Holocaust Survivors, Swiss Banks OK Settlement*, L.A. TIMES (Jan. 23, 1999), http://articles.latimes.com/1999/jan/23/news/mn-891 [https://perma.cc/9524-2FUL] (detailing settlement in class action lawsuit by Holocaust survivors against Swiss banks).

92 For a Swiss government explanation of Switzerland's neutrality, see STEFAN AESCHIMANN ET AL., FED. DEP'T OF DEF., CIVIL PROT. & SPORTS & FED. DEP'T OF FOREIGN AFFAIRS, SWISS NEUTRALITY (4th rev. ed.), https://www.eda.admin.ch/content/dam/eda/en/documents/aussenpolitik/voelkerrecht/Swiss%20neutrality.pdf [https://perma.cc/9MW9-SCSG]. In discussing World War II, the report concludes that Switzerland "[a]pplied a policy of neutrality," but notes, with dramatic understatement, that "[i]n retrospect, Switzerland's refugee policy should have been more generous." *Id.* at 18.

93 Microsoft's proposal of the Digital Switzerland framing can be understood as an implicit claim to parity. Facebook has been explicit. *See* KIRKPATRICK, *supra* note 19, at 254 ("In a lot of ways Facebook is more like a government than a traditional company." (quoting Facebook CEO Mark Zuckerberg)).

94 *See, e.g.*, *supra* note 18 (collecting sources analogizing companies to states).

95 Part III takes up the question of whether it is normatively desirable.

vast majority of countries worldwide. Facebook's 1.47 billion active daily users[96] surpasses the population of China (1.38 billion),[97] and Microsoft Office's 1.2 billion users[98] nearly equals the population of India (1.30 billion).[99] Google's Gmail too has over 1 billion active users per month.[100] Even Apple, which has only around half the user base of the companies just discussed, is estimated to have 588 million users around the world.[101] The user bases of *any* of these companies would place the company at least third on a ranking of countries by population.[102] The population of the United States (329.3 million)[103] now falls just behind the number of active monthly users of Twitter (330 million).[104]

The point of these comparisons is to put into perspective the extent of the impact a policy change by one of these companies has. To be sure, the companies exercise significantly thinner power over individuals than territorial sovereigns do. Nonetheless, with the exception of China and India, the number of people directly affected by a governmental policy change pales in comparison to the number subject to regulation by even one of the companies discussed, and many people use multiple companies' products and services. In at least this sense, the choice of Switzerland as the country comparator for the technology companies dramatically undersells their reach: Switzerland's population is just over 8 million.[105]

Indeed, the choice to analogize to *any* single country glosses over one of the companies' main sources of power: their transnational reach. Unlike countries, they are not confined within a single state. To better capture this feature, a

---

96 *Stats*, FACEBOOK: NEWSROOM, https://newsroom.fb.com/company-info [https://perma.cc/Y8PZ-HUTU?type=image] (last visited Feb. 8, 2019) (reporting statistic for June 2018).

97 *The World Factbook: China*, CENT. INTELLIGENCE AGENCY, https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html [https://perma.cc/5QYY-CKMS] (last updated Jan. 28, 2019).

98 Brian Fung, *Microsoft Is Adding LinkedIn to Its Professional Network*, WASH. POST (June 13, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/06/13/microsoft-is-about-to-add-linkedin-to-its-professional-network [https://perma.cc/5TBJ-QB2].

99 *The World Factbook: India*, CENT. INTELLIGENCE AGENCY, https://www.cia.gov/library/publications/the-world-factbook/geos/in.html [https://perma.cc/DRR7-MV4Y] (last updated Feb. 5, 2019).

100 *See* Alyson Shontell, *Gmail Now Has More than 1 Billion Monthly Active Users, Along with 6 Other Google Products*, BUS. INSIDER (Feb. 1, 2016, 5:12 PM), http://www.businessinsider.com/gmail-has-1-billion-monthly-active-users-2016-2 [https://perma.cc/23GT-7HEW] (reporting statistics provided by Google CEO Sundar Pichai in an Alphabet earnings call).

101 Kif Leswing, *Investors Are Overlooking Apple's Next $50 Billion Business*, BUS. INSIDER (Apr. 4, 2016, 2:10 PM), http://www.businessinsider.com/credit-suisse-estimates-588-million-apple-users-2016-4 [https://perma.cc/Z5EW-4AU7].

102 *The World Factbook: Country Comparison: Population*, CENT. INTELLIGENCE AGENCY, https://www.cia.gov/library/publications/the-world-factbook/rankorder/2119rank.html#us [https://perma.cc/33FW-BX36] (last visited Feb. 8, 2019).

103 *The World Factbook: United States*, CENT. INTELLIGENCE AGENCY, https://www.cia.gov/library/publications/the-world-factbook/geos/us.html [https://perma.cc/M9DL-LECA] (last updated Jan. 22, 2019).

104 Twitter, Inc., Annual Report (Form 10-K) 46 (Feb. 23, 2018) [hereinafter Twitter 10-K].

105 *The World Factbook: Switzerland*, CENT. INTELLIGENCE AGENCY, https://www.cia.gov/library/publications/the-world-factbook/geos/sz.html [https://perma.cc/LY63-HC8W] (last updated Jan. 29, 2019).

non-nation-state analogy might be more apt—something like a religion with global adherents or a nongovernmental organization like the International Committee of the Red Cross—though those analogies too would have flaws.

Financial Resources. The comparison between the financial resources of countries and powerful U.S. technology companies is not quite as dramatic as the comparison of populations and user bases, but it is still striking. In a 2016 study, the nongovernmental organization Global Justice Now compared the annual revenues of countries and corporations.[106] In a ranking of the top 100 governments and corporations by revenue,[107] only 30 countries made the list, as compared to 70 corporations.[108] Apple was the top technology company, ranked 25th, just behind India and several slots ahead of Switzerland.[109] The top 100 included other U.S. technology companies, such as Amazon (73rd), HP (77th), and Microsoft (92nd).[110] Other technology companies were slightly further down the rankings. Alphabet, Google's parent company, came in at 132nd, just behind Israel (130th).[111]

Public Roles and Policy Proposals. In addition to the companies' characteristics, their actions also suggest a self-conception of parity with governments. Put simply, they act like governments in some circumstances.

U.S. technology companies have taken on some arguably public functions related to foreign policy and crime control.[112] They have thwarted (or at least attempted to thwart) government cyber operations.[113] One way they have

---

106 *10 Biggest Corporations Make More Money than Most Countries in the World Combined*, GLOB. JUSTICE NOW (Sept. 12, 2016), http://www.globaljustice.org.uk/news/2016/sep/12/10-biggest-corporations-make-more-money-most-countries-world-combined [https://perma.cc/GWC9-AMDZ] (explaining that the annual revenue figures were taken from the CIA World Factbook for countries and from the Fortune Global 500 for companies).

107 *Corporations vs Governments Revenues: 2015 Data*, GLOB. JUSTICE NOW (Sept. 12, 2016), http://www.globaljustice.org.uk/sites/default/files/files/resources/corporations_vs_governments_final.pdf [https://perma.cc/L7W3-WRNG]; *see also* Duncan Green, *The World's Top 100 Economies: 31 Countries; 69 Corporations*, THE WORLD BANK: PEOPLE, SPACES, DELIBERATION (Sept. 20, 2016), http://blogs.worldbank.org/publicsphere/world-s-top-100-economies-31-countries-69-corporations [https://perma.cc/H5HQ-2PQU] (reporting rankings of corporations and governments by Global Justice Now).

108 Phillip Inman, *Study: Big Corporations Dominate List of World's Top Economic Entities*, GUARDIAN (Sept. 12, 2016, 10:41 EDT), https://www.theguardian.com/business/2016/sep/12/global-justice-now-study-multinational-businesses-walmart-apple-shell [https://perma.cc/5NWV-V9JD].

109 *Corporations vs Governments Revenues: 2015 Data*, *supra* note 107.

110 *Id.* Companies outside the technology sector place even higher on the list. *See id.* (listing, for example, Walmart 15th and Royal Dutch Shell 18th).

111 *Id.*

112 For a fuller exploration of why these actions constitute public functions, see Eichensehr, *supra* note 74, at 475-78.

113 *See, e.g.*, Kevin Poulsen, *Putin's Hackers Now Under Attack—From Microsoft*, DAILY BEAST (July 20, 2017, 10:05 PM ET), http://www.thedailybeast.com/microsoft-pushes-to-take-over-russian-spies-network [https://perma.cc/S2R7-J69Q] (discussing lawsuit filed by Microsoft to take control of command-and-control servers used by Russian government hackers); *see also* Report & Recommendation at 16, Microsoft

done so is by warning individuals who are targeted by state-sponsored actors.[114] Another is through coordinated action to remove malware infections that state actors use to spy on targets.[115]

An interesting example occurred in 2014. In a report titled *Operation SMN*, a coalition of companies, including Cisco, FireEye, iSight Partners, Microsoft, and Novetta, explained that they had discovered that the "Axiom" group—"part of [the] Chinese Intelligence Apparatus"[116]—had spied on "numerous Fortune 500 companies, journalists, environmental groups, pro-democracy groups, software companies, academic institutions, and government agencies worldwide" for several years.[117] To address the threat, the companies shared threat information with "trusted industry partners" around the world, with the result that "over 43,000 separate installations of Axiom-related tools [were] removed from machines protected by Operation SMN partners."[118] The operation was significant because it was entirely industry led, designed, and executed.[119] A representative of one of the companies involved explained that Operation SMN is "'the beginning of . . . industry-coordinated efforts to expose these threat groups, and to do so without having to use law enforcement, to help corporations and governments around the world combat' hackers."[120]

Companies also engage in cybercrime control efforts. Microsoft in particular has undertaken a number of "botnet takedowns."[121] "Botnets" are

---

Corp. v. John Does 1-2, No. 1:16-cv-993 (E.D. Va. Aug. 1, 2017) (recommending that Microsoft's motion for default judgment and permanent injunction be granted).

114 *See supra* notes 34–41 and accompanying text.

115 More recently, private parties have collaborated to address government-sponsored use of platforms to spread misinformation and promote division. *See, e.g.*, Kate Conger & Sheera Frenkel, *How FireEye Helped Facebook Spot a Disinformation Campaign*, N.Y. TIMES (Aug. 23, 2018), https://www.nytimes.com/2018/08/23/technology/fireeye-facebook-disinformation.html (discussing collaboration to remove accounts linked to Russian and Iranian state actors).

116 NOVETTA, OPERATION SMN: AXIOM THREAT ACTOR GROUP REPORT 4 (2014), http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf [https://perma.cc/2NGM-7EAX].

117 *Id*. For additional analysis of the report, see Kristen Eichensehr, *The Private Frontline in Cybersecurity Offense and Defense*, JUST SEC. (Oct. 30, 2014), https://www.justsecurity.org/16907/private-frontline-cybersecurity-offense-defense [https://perma.cc/N5UG-PVDJ].

118 NOVETTA, *supra* note 116, at 5-6.

119 *See* DJ Summers, *As Cyber Attacks Swell, a Move Toward Improved Industry Collaboration*, FORTUNE (Jan. 7, 2015), http://fortune.com/2015/01/07/cybersecurity-collaboration [https://perma.cc/HZL2-J6KW] ("Operation SMN marks the first time that computer security players . . . are bonding without using federal or international law enforcement agencies as glue.").

120 Ellen Nakashima, *Researchers Identify Sophisticated Chinese Cyberespionage Group*, WASH. POST (Oct. 28, 2014), https://www.washingtonpost.com/world/national-security/researchers-identify-sophisticated-chinese-cyberespionage-group/2014/10/27/de30bc9a-5e00-11e4-8b9e-2ccdac31a031_story.html [https://perma.cc/JG99-CX3P] (quoting Stephen Ward, Senior Director, iSight Partners).

121 *See* BOTNET LEGAL NOTICE, http://www.botnetlegalnotice.com [https://perma.cc/US5N-CP3K] (last visited Feb. 8, 2019) (collecting court filings and orders related to various takedowns in which Microsoft has been involved). Microsoft is the most prominent, but not the only, company that has engaged in takedown

networks of computers infected with malicious software that allows them to be controlled remotely and used for a variety of activities, including denial of service attacks, spam distribution, and fraud.[122] To stop botnets, Microsoft has filed numerous civil lawsuits in federal district courts against botnet operators, arguing that botnets that use Microsoft products harm Microsoft and its customers and raising claims of unauthorized access to protected computers and trademark infringement.[123] Courts have permitted Microsoft to seize control of and effectively deactivate botnets.[124] Microsoft used similar legal theories in a lawsuit to disrupt Russian government election-related hacking.[125] The resort to the court system to effectuate these endeavors does not render them less state-like: when the U.S. government has done botnet takedowns, it has similarly filed civil suits to obtain court orders allowing it to seize control of botnet infrastructure.[126] In its crime control efforts, Microsoft is acting like U.S. federal law enforcement.[127]

In recent years, companies have also begun to make public policy proposals, and not just any proposals: ones that would systematically elevate the role of companies and other nongovernmental actors and decrease the role of

operations. *See, e.g.*, Michael Mimoso, *Facebook Carries Out Lecpetex Botnet Takedown*, THREATPOST (July 9, 2014, 11:08 AM), http://threatpost.com/facebook-carries-out-lecpetex-botnet-takedown/107096 [https://perma.cc/LWG5-YQ5S] (describing Facebook's takedown of a botnet).

122 *See, e.g.*, *What Is a Botnet?*, NORTON, https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html [https://perma.cc/GRP6-RDJZ] (last visited Feb. 8, 2019) (describing botnets in general); *see also* Lily Hay Newman, *What We Know About Friday's Massive East Coast Internet Outage*, WIRED (Oct. 21, 2016, 1:04 PM), https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn [https://perma.cc/PM3N-HHKP] (discussing the Mirai botnet that was used in a distributed denial of service (DDOS) attack against Dyn).

123 *See, e.g.*, Complaint at 11-12, Microsoft Corp. v. John Does 1-5, No. 15-cv-06565 (E.D.N.Y. Nov. 23, 2015) (discussing how the Dorkbot botnet harms Microsoft and its customers); *id.* at 13-15 (raising unauthorized access and trademark-related claims).

124 *See, e.g.*, Order Granting Default Judgment & Permanent Injunction, Microsoft Corp. v. John Does 1-82 at 9-12, No. 3:13-cv-00319 (W.D.N.C. Nov. 21, 2013) (granting Microsoft a permanent injunction and transferring ownership of malicious domains to Microsoft). In some cases, Microsoft works with government officials in takedown operations. *See, e.g.*, Press Release, Europol, Andromeda Botnet Dismantled in International Cyber Operation (Dec. 4, 2017), https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation [https://perma.cc/4APS-RGCM] (detailing cooperation by U.S. and foreign law enforcement and Microsoft to take down the Andromeda botnet).

125 *See supra* note 113; *see also* Lily Hay Newman, *How Microsoft Tackles Russian Hackers—And Why It's Never Enough*, WIRED (Aug. 21, 2018, 3:11 PM), https://www.wired.com/story/microsoft-russia-fancy-bear-hackers-sinkhole-phishing [https://perma.cc/M9BP-K7L5] (discussing Microsoft's suit permitting it to seize domains and sinkhole traffic); David E. Sanger & Sheera Frenkel, *New Russian Hacking Targeted Republican Groups, Microsoft Says*, N.Y. TIMES (Aug. 21, 2018), https://www.nytimes.com/2018/08/21/us/politics/russia-cyber-hack.html (reporting that Microsoft discovered websites designed to mimic Republican groups and that a court-appointed special master permitted Microsoft to "seize fake websites as soon as they are registered").

126 *See* Eichensehr, *supra* note 74, at 480 (discussing the Coreflood botnet takedown).

127 Sometimes Microsoft has acted not just like, but with, federal law enforcement. *See id.* at 480-81 (discussing public–private collaboration on the Citadel and ZeroAccess botnet takedowns).

governments. For example, Microsoft has proposed the establishment of an international institution to handle attribution of cyberattacks to nation-states.[128] Microsoft suggests modeling the institution on the International Atomic Energy Agency and having its membership "consist of technical experts from across governments, the private sector, academia, and civil society with the capability to examine tactics, techniques, and procedures used by nation-state attackers, as well as indicators of compromise that suggest a given attack was by a nation-state."[129] Experts have raised questions about the feasibility of the proposal, but also acknowledge that such a body could "help to a considerable extent address the politicization of many attribution judgments today."[130] A recent Microsoft-funded study by the RAND Corporation went further, proposing a Global Cyber Attribution Consortium that would entirely exclude governments.[131]

Even more recently, as the culmination of a push by Microsoft President Brad Smith, more than sixty tech companies from the United States and Western Europe signed a Cybersecurity Tech Accord.[132] The Accord commits the companies to "strive to protect all of [their] users and customers from cyberattacks . . . irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical."[133] The signatories also vow that they "will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere."[134] Signatories

128 SCOTT CHARNEY ET AL., MICROSOFT, FROM ARTICULATION TO IMPLEMENTATION: ENABLING PROGRESS ON CYBERSECURITY NORMS 11-12 (2016), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8 [https://perma.cc/H57G-GR46].

129 *Id.* at 11.

130 Herb Lin, *Microsoft Proposes an Independent Body for Making Attribution Judgments*, LAWFARE (June 24, 2016, 3:50 PM), https://www.lawfareblog.com/microsoft-proposes-independent-body-making-attribution-judgments [https://perma.cc/D53U-6WAL].

131 JOHN S. DAVIS II ET AL., RAND CORP., STATELESS ATTRIBUTION: TOWARD INTERNATIONAL ACCOUNTABILITY IN CYBERSPACE vi, 27, 30-31 (2017), https://www.rand.org/pubs/research_reports/RR2081.html [https://perma.cc/4BWC-VXXW].

132 *About Cybersecurity Tech Accord*, CYBERSECURITY TECH ACCORD, https://cybertechaccord.org/about [https://perma.cc/W9D8-GZ8T] (last visited Feb. 8, 2019); *see also* Chris Bing, *Microsoft-Led Industry Group Pledges to Not Assist Government Cyberattacks*, CYBERSCOOP (Apr. 17, 2018), https://www.cyberscoop.com/microsoft-brad-smith-cyber-norms-rsa-2018 [https://perma.cc/4PT3-6JN4] (describing the Accord and noting that Microsoft led the effort to gain agreement from other companies); Sanger, *supra* note 79 ("The impetus for the effort came largely from Mr. Smith, who has been arguing for several years that the world needs a 'digital Geneva Convention' that sets norms of behavior for cyberspace . . . .").

133 *Cybersecurity Tech Accord*, CYBERSECURITY TECH ACCORD, https://cybertechaccord.org/accord [https://perma.cc/Y586-QBN8] (last visited Feb. 8, 2019).

134 *Id.*; *see* Sanger, *supra* note 79 (noting that this commitment "reflect[s] Silicon Valley's effort to separate itself from government cyberwarfare"). The Accord preserves, however, some flexibility. For example, who determines who counts as an "innocent" civilian? *Cf.* SANGER, *supra* note 42, at 306-07 (praising the Accord but raising critiques, including that the wording "left lots of maneuvering room for the companies to join attacks against terror groups, or even against governments repressing their own citizens").

include Cisco, Microsoft, Facebook, FireEye, and Symantec, as well as Nokia from Finland and Telefónica from Spain.[135]

When considered based on the size of their "constituencies," financial resources, and ability to counter criminal and governmental cyberthreats, the comparison between major U.S. technology companies and countries seems not unfounded. There is no doubt that the companies are both powerful and sophisticated actors in the international sphere.

Motivations. In addition to these practical similarities to states, the technology companies may be similar to governments in a more theoretical way as well, namely in the mixed motivations that drive their actions. The companies, like states, are multimember entities, with different internal actors pushing along the ship of "state." Differing motivations drive different—and competing—internal actors who in turn shape company behavior and may push the companies to act consistent with the Digital Switzerlands idea.

One possible explanation for the companies' behavior is economic: the companies may assess that the posture of neutrality will best maximize their growth and profits going forward by increasing their appeal to users worldwide.[136] Economic incentives are certainly at play in virtually all company behavior. For corporate officers, ignoring the companies' economic interests would be a dereliction of duties to shareholders.[137] But this realist account isn't the only possible explanation or necessarily a total one.

A competing explanation would focus on the moral and normative commitments of individuals within the companies: when important corporate decisionmakers or other employees who play key roles are personally committed to values like user privacy or transparency, they can drive the company, for example, to resist government demands to weaken privacy.[138]

---

135 Sanger, *supra* note 79; *Signing Pledge to Fight Cyberattacks, 34 Leading Companies Promise Equal Protection for Customers Worldwide*, CYBERSECURITY TECH ACCORD (Apr. 17, 2018), https://cybertechaccord.org/signing-pledge-to-fight-attacks-cyber-accord [https://perma.cc/8AMD-YTA6].

136 *See* Government's Motion to Compel Apple Inc. to Comply with This Court's February 16, 2016 Order Compelling Assistance in Search at 2-3, *In re* the Search of an Apple Iphone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. CM 16-10 (C.D. Cal. Feb. 19, 2016) ("Apple's current refusal to comply with the Court's Order . . . appears to be based on its concern for its business model and public brand marketing strategy."); *cf.* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1627-30 (2018) (discussing the economic incentives that drive technology companies to implement content moderation policies that will meet user expectations).

137 *See, e.g.*, *Developments in the Law—More Data, More Problems*, *supra* note 60, at 1730 & n.51 (noting that for companies incorporated in Delaware, as many of the tech companies are, "generat[ing] profits for [their] shareholders . . . is . . . the bedrock principle that is supposed to animate every decision" (footnote omitted)).

138 *See* Eichensehr, *supra* note 74, at 503-04 (discussing the role of community attachments in motivating the behavior of corporate employees in cybersecurity); Finnemore & Hollis, *supra* note 14, at 461 (highlighting the "cultural norms" that "dispose technologists toward particular views of the role that digital technology can or should play in society"); Klonick, *supra* note 136, at 1618-22

Battles over public-law values are happening inside companies and appear to have prompted the resignation of at least one high-profile employee.[139]

Yet another explanation might focus on the culture of Silicon Valley and the effects on particular companies or decisionmakers within those companies of being embedded in a milieu that values privacy and security.[140]

Still another explanation might merge these possibilities, suggesting that companies sometimes act in accordance with the proprivacy, transparency, or other normative commitments of important employees to retain their loyalty and services, which in turn maximizes the companies' success in the long run. For example, a values-based push by Google employees for the company to cease work on artificial intelligence for a U.S. military targeting program led to resignations,[141]

(discussing how the First Amendment values held by technology company decisionmakers, especially lawyers, shape the companies' content moderation policies); Deirdre K. Mulligan & Kenneth A. Bamberger, *Saving Governance-by-Design*, 106 CALIF. L. REV. 697, 714-15 (2018) (discussing a "movement among engineers and designers to be more conscious of the values embedded in the systems they design" and "to address values more systematically in technical practice").

139 *See* Frenkel et al., *supra* note 18 (providing a detailed account of conflict within Facebook over security and election interference); Nicole Perlroth, Sheera Frenkel, & Scott Shane, *Facebook Exit Hints at Dissent on Handling of Russian Trolls*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-alex-stamos.html (reporting that Facebook's Chief Information Security Officer, Alex Stamos, made plans to leave the company after pushing unsuccessfully for "more disclosure around Russian interference of the platform" and explaining that "[o]ne central tension at Facebook has been" between the "security team[, which] generally pushed for more disclosure about how nation states had misused the site," and "the legal and policy teams[, which] have prioritized business imperatives"). Resignations as a tool to protest an entity's failure to live up to public values present another metasimilarity between tech companies and governments as resignation-in-protest is often associated with government officials. *See, e.g.*, David Johnston, *Bush Intervened in Dispute over N.S.A. Eavesdropping*, N.Y. TIMES (May 16, 2007), https://www.nytimes.com/2007/05/16/washington/16nsa.html (detailing an episode in which Justice Department officials threatened to resign rather than reauthorize a surveillance program); Oona Hathaway, *Work for the Trump Administration? Yes, but Be Prepared*, JUST SEC. (Nov. 14, 2016), https://www.justsecurity.org/34409/work-trump-administration-yes-prepared [https://perma.cc/65QE-FWLN] (discussing the "power of public servants to resign—publicly and prominently—when they are asked to formulate or implement abusive policies"). For an extended treatment of resignations in protest by government officials, see generally EDWARD WEISBAND & THOMAS M. FRANCK, RESIGNATION IN PROTEST: POLITICAL AND ETHICAL CHOICES BETWEEN LOYALTY TO TEAM AND LOYALTY TO CONSCIENCE IN AMERICAN PUBLIC LIFE (1975).

140 *See* Finnemore & Hollis, *supra* note 14, at 442 (identifying a "culture of Silicon Valley" that emphasizes security and privacy); *see also* RYAN GOODMAN & DEREK JINKS, SOCIALIZING STATES: PROMOTING HUMAN RIGHTS THROUGH INTERNATIONAL LAW 22 (2013) (identifying "material inducement" and "persuasion" as mechanisms that influence state behavior and proposing the addition of "acculturation," defined as "the process by which actors adopt the beliefs and behavioral patterns of the surrounding culture, without actively assessing either the merits of those beliefs and behaviors or the material costs and benefits of conforming to them").

141 *See* Kate Conger, *Google Employees Resign in Protest Against Pentagon Contract*, GIZMODO (May 14, 2018, 6:00 AM), https://gizmodo.com/google-employees-resign-in-protest-against-pentagon-con-1825729300 [https://perma.cc/ARN8-YQMH]; *see also* Scott Shane & Daisuke Wakabayashi, *'The Business of War': Google Employees Protest Work for the Pentagon*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html (noting that more than 3000 employees

and ultimately Google backed down, announcing that it would not renew the contract.[142]

Consideration of values-based explanations for the companies' behavior is thus fully consistent with a realist explanation focused on the companies' economic interests. Like the Swiss neutrality on which it is modeled, the Digital Switzerlands idea is partly principled and partly strategic. Principle and strategy can point in the same direction: taking actions to maintain long-term trust in the digital ecosystem encourages greater use of the Internet and the companies' products, while also supporting ideological commitments to privacy and security.

All of these possibilities (and probably others) have some purchase, but none has a monopoly on explanatory value. And this mixture of possible or partial explanations for company behavior should not be surprising. International relations and international law scholars have long debated how best to explain state behavior, particularly diverging on the extent to which states are driven by interests versus ideas.[143] The existence of similar competing or complementary explanations—profit interests versus privacy ideals—for companies adds further impetus to take seriously the company-to-sovereign analogy. At the same time, however, the persistence of theoretical debates about state behavior suggests that a definitive resolution to similar debates about technology companies will also remain elusive.[144]

---

signed a letter to Google's CEO protesting Google's work for the Pentagon and explaining that although "[a]n uneasiness about military contracts among a small fraction of Google's more than 70,000 employees may not pose a major obstacle to the company's growth[,] . . . in the rarefied area of artificial intelligence research, Google is engaged in intense competition . . . for the most talented people").

142 Daisuke Wakabayashi & Scott Shane, *Google Will Not Renew Pentagon Contract that Upset Employees*, N.Y. TIMES (June 1, 2018), https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html. The companies' positions on work for the U.S. military vary. *See, e.g.*, David E. Sanger, *Microsoft Says It Will Sell Pentagon Artificial Intelligence and Other Advanced Technology*, N.Y. TIMES (Oct. 26, 2018), https://www.nytimes.com/2018/10/26/us/politics/ai-microsoft-pentagon.html (reporting that, unlike Google, Microsoft will compete for a Pentagon cloud computing contract and that Microsoft President Brad Smith "would not indicate whether Microsoft would also provide all of its products to, say, the [Chinese] People's Liberation Army," saying only that "'It's an issue we are going to have to work through'" (quoting Brad Smith)); Nitasha Tiku, *Amazon's Jeff Bezos Says Tech Companies Should Work with the Pentagon*, WIRED (Oct. 15, 2018, 5:13 PM), https://www.wired.com/story/amazons-jeff-bezos-says-tech-companies-should-work-with-the-pentagon [https://perma.cc/PJ9V-NVBM] ("If big tech companies are going to turn their back on [the] US Department of Defense, this country is going to be in trouble." (quoting Amazon CEO Jeff Bezos)).

143 *See* OONA A. HATHAWAY & HAROLD HONGJU KOH, FOUNDATIONS OF INTERNATIONAL LAW AND POLITICS 111 (2005) ("How and why ideas matter, and the extent to which they influence international relations and international law, remains a source of disagreement."). For overviews of competing theories, see, for example, Peter J. Katzenstein, Robert O. Keohane & Stephen D. Krasner, *International Organization and the Study of World Politics*, 52 INT'L ORG. 645, 657-78 (1998), and Richard H. Steinberg & Jonathan M. Zasloff, *Power and International Law*, 100 AM. J. INT'L L. 64, 71-85 (2006).

144 *See, e.g.*, Steinberg & Zasloff, *supra* note 143, at 86 ("None of the metatheories of the last century have been able to deliver the knockout blow that some may have once thought possible. No

Where Parity Falls Short. Despite these similarities to states, the companies still lack core attributes of sovereignty traditionally understood to define the essence of statehood.

One classic definition of a state is Max Weber's: "[A] state is a human community that (successfully) claims the *monopoly of the legitimate use of physical force* within a given territory."[145] Territory, according to Weber, "is one of the characteristics of the state."[146] And it is one that the companies lack.[147] Some have massive headquarters complexes,[148] but all are located within sovereign states. The relevant monopolizers of legitimate use of physical force are governments, not the companies.

Another key feature of states is sovereignty.[149] Although "sovereignty has always been a plastic norm in practice,"[150] Stephen Krasner has identified four distinct types of sovereignty:[151] (1) "International legal sovereignty" encompasses "the practices associated with mutual recognition, usually between territorial entities that have formal juridical independence";[152] (2) "Westphalian sovereignty refers to political organization based on the exclusion of external actors from authority structures within a given

one trying to understand international relations can ignore power, *or* law, *or* the state, *or* civil society, *or* norms, *or* language.").

145 MAX WEBER, *Politics as a Vocation*, *in* FROM MAX WEBER: ESSAYS IN SOCIOLOGY 77, 78 (H.H. Gerth & C. Wright Mills eds., trans., Oxford Univ. Press 1958). This, of course, is not the only possible definition of statehood. *See, e.g.*, Chander, *supra* note 18, at 1817-19 (comparing Facebook to the international law criteria for a state, as set out in Article 1 of the Montevideo Convention on Rights and Duties of States, including that it "possess . . . : (a) a permanent population; (b) a defined territory; (c) government; and (d) capacity to enter into relations with the other states" (internal quotation marks omitted)). The definitions, however, are largely overlapping, creating similar ways across definitions in which the tech companies may meet and fail in equivalence with states.

146 WEBER, *supra* note 145, at 78.

147 *See* Chander, *supra* note 18, at 1817 ("Facebook obviously lacks . . . a defined territory."). *But see* Cohen, *supra* note 18, at 200 ("[P]latforms have both territories and populations. Platform territories are not contiguous physical spaces but rather are defined using protocols, data flows, and algorithms. Both technically and experientially, however, they are clearly demarcated spaces with virtual borders that platforms guard vigilantly.").

148 *See, e.g.*, Julie Balise, *Office Space: Google's Campus Feels as Big as the Internet Itself*, SFGATE (Jan. 5, 2015, 1:23 PM PST), http://www.sfgate.com/business/article/Office-Space-Google-s-campus-feels-as-big-as-5992389.php [https://perma.cc/5AZ9-2QCN?type=image] (describing Google's Bay-area headquarters and noting its size as "[b]ig, but Google wouldn't say how big"); Jennifer Warnick, *88 Acres: How Microsoft Quietly Built the City of the Future*, MICROSOFT, https://www.microsoft.com/en-us/stories/88acres [https://perma.cc/73RY-RZ3T] (last visited Feb. 8, 2019) (noting that Microsoft's campus in Redmond, Washington now encompasses 500 acres).

149 *See* STEPHEN D. KRASNER, SOVEREIGNTY: ORGANIZED HYPOCRISY 220 (1999) ("The bundle of properties associated with sovereignty—territory, recognition, autonomy, and control—have been understood, often implicitly, to characterize states in the international system.").

150 Kal Raustiala, *Sovereignty and Multilateralism*, 1 CHI. J. INT'L L. 401, 401 (2000).

151 KRASNER, *supra* note 149, at 3; *see id.* at 9-25 (explaining the four conceptions of sovereignty).

152 *Id.* at 3.

territory";[153] (3) "[d]omestic sovereignty refers to the formal organization of political authority within the state and the ability of public authorities to exercise effective control within the borders of their own polity";[154] and (4) "interdependence sovereignty refers to the ability of public authorities to regulate the flow of information, ideas, goods, people, pollutants, or capital across the borders of their state."[155] These characteristics of sovereignty are often honored only in the breach, and as Krasner himself notes, "only a very few states have possessed all of these attributes."[156]

The fact that states can survive and continue to be recognized as states even absent some of the characteristics of sovereignty is, however, little help to the companies. To date, the companies possess *none* of these types of sovereignty. Countries do not recognize them as states, and they lack "juridical independence."[157] They lack authority to exclude governmental officials from their premises. They are also subordinate to public authorities and legal regimes within the states in which they operate. They may come closest to possessing interdependence sovereignty: the companies cannot regulate *all* information, goods, or people that cross an international border—such borders are not theirs to police. But considered from the perspective of individuals, the companies may effectively represent a supplemental sovereign, in addition to the territorial sovereign.[158]

* * *

Companies approach parity with states on some aspects of practical power. They have enormous user bases and state-like financial resources, and they have begun *acting* like states, engaging in crime control and public policy. Explaining their motivations also poses challenges similar to those that have long bedeviled theorists of state behavior. But the companies lack the formal attributes of statehood and sovereignty. They do not possess sovereign

153 *Id.* at 3-4; *see also* Jack Goldsmith & Daryl Levinson, *Law for States: International Law, Constitutional Law, Public Law*, 122 HARV. L. REV. 1791, 1845 (2009) ("In international law, 'sovereignty' signifies the idea that a state or a nation exercises effective and supreme control within a territory and is formally independent of any external or superior authority structure, including other states and international organizations.").

154 KRASNER, *supra* note 149, at 4.

155 *Id.*

156 *Id.* at 220.

157 *Id.* at 3.

158 *See infra* Section III.A (discussing the effect of multiple "sovereigns"); *cf.* Pasquale, *supra* note 6 (arguing, based on a domestic context, that "major digital firms . . . aspire to displace more government roles over time, replacing the logic of territorial sovereignty with functional sovereignty").

territory, are not recognized by sovereigns as sovereign, and remain subject to the overriding public authorities in countries where they operate.[159]

Those features may, of course, evolve. On the recognition-by-states-as-states front, the companies have employees that function as ambassadors to governments,[160] and one country—Denmark—has appointed a diplomat as "tech ambassador," resident in Silicon Valley.[161] In announcing the tech ambassador position, Danish Foreign Minister Anders Samuelsen explained that the U.S. technology companies "affect Denmark just as much as entire countries" and "have become a type of new nations."[162]

B. *Neutrality*

The second idea embedded in the "Digital Switzerland" concept is that the technology companies are not just akin to countries but to *neutral* countries.

Even more than the claim of parity, promoting the idea of their own neutrality serves the companies' interests. The markets for the companies' products are increasingly international. For a number of the companies, the majority of their revenue already comes from non-U.S. sources.[163] For 2017, for example, Alphabet (Google's parent company) derived only with 47% of its revenue from the United

---

159 *Cf.* SEGAL, *supra* note 44, at 27 ("Nation-states still regulate the companies that create the hardware and software of cyberspace; threaten, imprison, fine, and monitor individual users; develop competing technology standards; and require that the physical infrastructure of the Internet be configured to give them more control.").

160 *See* Cyrus Farivar, *Mr. Ambassador, Meet President Zuckerberg*, SLATE (May 27, 2011, 12:31 PM), http://www.slate.com/articles/technology/technology/2011/05/mr_ambassador_meet_president_zuckerberg.html [https://perma.cc/643Y-EMFS] (reporting that Facebook and Google have sent employees to act as emissaries to foreign governments).

161 *See Denmark Names First Ever Digital Ambassador for Silicon Valley Role*, LOCAL (Den.) (May 26, 2017, 18:02 CEST), https://www.thelocal.dk/20170526/denmark-names-first-ever-digital-ambassador-for-silicon-valley-role [https://perma.cc/GJ8U-XT4J] (reporting the appointment of Denmark's ambassador to Indonesia, Casper Klynge, as the "tech ambassador"). Such diplomacy is not one sided. *See* Cohen, *supra* note 18, at 202 ("Platforms . . . increasingly practice diplomacy in the manner of sovereign actors. Facebook's privacy team travels the world meeting with government officials to determine how best to satisfy their concerns while continuing to advance Facebook's own interests, much as a secretary of state and his or her staff might do.").

162 Robbie Gramer, *Denmark Creates the World's First Ever Digital Ambassador*, FOREIGN POL'Y (Jan. 27, 2017, 2:37 PM), http://foreignpolicy.com/2017/01/27/denmark-creates-the-worlds-first-ever-digital-ambassador-technology-europe-diplomacy [https://perma.cc/5KGX-NUXY] (quoting interview with Samuelsen in *Politiken*, a Danish newspaper).

163 Twitter is an exception. In 2017, Twitter's total revenue amounted to $2.44 billion, of which $1.41 billion (57.79%) came from the United States. Twitter 10-K, *supra* note 104, at 46. Microsoft's U.S.-derived revenue hovers around 50%. For the fiscal year ending in June 2016, 47.6% of Microsoft's revenue came from the United States. *See, e.g.*, Microsoft Corp., Annual Report (Form 10-K) 93 (July 28, 2016) (showing total revenue for fiscal year 2016 of $85,320 million, of which only $40,578 million (or 47.6%) came from the United States). The percentage has increased slightly since then. *See* Microsoft Corp., Annual Report (Form 10-K) 94 (Aug. 3, 2018) (showing total revenue for fiscal year 2018 of $110,360 million, of which $55,926 million (or 50.7%) came from the United States).

States.[164] For Apple, the comparable figures are even lower: only 36.8% of Apple's net sales revenue came from the United States for the fiscal year ending in September 2017.[165] The markets for the companies' products are also not just private parties. The companies do business with governments around the world.[166]

If market is considered based on user location rather than revenue, it is equally true that the markets for the companies' products are more international than domestic. In December 2017, Facebook had 2.13 billion monthly active users, of whom only 239 million came from the United States or Canada,[167] and Twitter had 330 million monthly active users, of whom only 68 million were in the United States.[168]

The markets are also likely to be increasingly international. As Adam Segal put it, "the future of cyberspace is not American, at least in terms of its users."[169] The growth potential for Internet users and smartphone owners outside the United States is far higher than within the United States. For example, Asia includes 55.1% of the world's population, but the Internet penetration rate there (the percentage of the population that uses the Internet) is only 49%, suggesting that there is an enormous population of potential Internet users who have yet to connect.[170] North America, by contrast, contains 4.8% of the world's population and already has an Internet penetration rate of 95%, meaning a far smaller pool of potential Internet users could come online there going forward.[171]

---

164 Alphabet Inc., Annual Report (Form 10-K) 32 (Feb. 6, 2018); *see also id.* at 27 (showing revenues of $52.4 billion from the United States, out of a total of $110.9 billion, and explaining that of the $110.9 billion, $109.7 billion derives from Google).

165 *See* Apple Inc., Annual Report (Form 10-K) 68 (Nov. 3, 2017) (showing $84,339 million in net sales from the United States out of a total of $229,234 million in net sales in 2017 (36.8%)).

166 *See, e.g.*, Kris Cheng, *Gov't to Continue Using Microsoft Email System Instead of Chinese One After Contract Granted to Shenzhen Firm*, H.K. FREE PRESS (May 9, 2018, 20:49), https://www.hongkongfp.com/2018/05/09/govt-continue-using-microsoft-email-system-instead-chinese-one-contract-granted-shenzhen-firm [https://perma.cc/3Q2W-XBMS] (reporting that the Hong Kong government uses Microsoft Exchange for email); Media Release, Nat'l Treasury, S. Afr., Office of the Chief Procurement Officer Join Forces to Reduce Costs and Enhance Efficiency in the Public Sector (Dec. 9, 2016), http://www.treasury.gov.za/comm_media/press/2016/20161212 01%20Media%20release%20Microsoft%20SITA%20TREASURY.pdf [https://perma.cc/FCD4-EXAS] (noting renegotiation of South African government contracts with Microsoft); Dara Kerr, *Apple Lands $159M Government Contract for iPhone, iPad*, CNET (Feb. 14, 2013, 5:13 PM PST), https://www.cnet.com/news/apple-lands-159m-government-contract-for-iphone-ipad (reporting Apple contract with New Zealand police).

167 Facebook provides an aggregate figure for the United States and Canada. *See* Facebook, Inc., Annual Report (Form 10-K) 36 (Feb. 1, 2018).

168 Twitter 10-K, *supra* note 104, at 47.

169 SEGAL, *supra* note 44, at 35.

170 World Internet Users and 2018 Population Stats, INTERNET WORLD STATS, http://www.internetworldstats.com/stats.htm [https://perma.cc/3WUB-Z5MY] (last updated June 30, 2018).

171 *Id.*; *cf. Governing Intelligence*, *supra* note 64, at 19:20 (statement of Scott Charney, Corporate Vice President, Microsoft Corp.) ("[Four-point-five] percent—that is the percentage of the world population in the United States. The next two billion people coming online will not be here."). For

The evolving demographics of the companies' customer and user bases drive the companies' apparent desire (or perceived need) to treat all governments equally. To appeal to the international users who will be key to their future growth, the U.S. technology companies are trying to shed or at least significantly downplay their origins and continued legal personality as *U.S.* companies. Instead, they cast themselves as neutrals amidst competing claims by national governments and in the face of claims by the U.S. government for preferential treatment because of their status as U.S. companies.

For example, in resisting a court order requiring it to write code to allow the FBI to access the iPhone of one of the San Bernardino shooters, Apple argued that it could not comply with the U.S. government's demand without acceding to similar requests from other governments.[172] In other words, to maintain its neutrality, Apple could not (even if it wanted to) do something that would be perceived as exceptional for the U.S. government. Treating the U.S. government in an exceptional manner would doom the company in international markets or put it in the position of having to grant all governments the same type of assistance and access—an option Apple rejected on security grounds.[173]

Microsoft officials have made similar arguments. Microsoft Corporate Vice President Scott Charney argued: "[W]hen one country attacks another country, . . . for us, that's one customer attacking another customer. And either customer might ask us for support and help."[174] Charney argued that in that circumstance, Microsoft has "to be Switzerland" and "do defense and not offense."[175] Brad Smith's RSA speech echoes a similar argument for resisting demands, even by a company's national government. Smith argued: "[W]e will not aid in attacking customers anywhere, *regardless of the government that may ask us to do so*."[176]

The recent Cybersecurity Tech Accord also reflects this concept of neutrality as a lack of exceptionalism. The signatory companies pledge not to help governments launch cyberattacks, full stop, with no carveout for the United States or other governments.[177] And their commitment to protect users who suffer attacks "irrespective of . . . the motives of the attacker,

---

statistics on Internet penetration rates, broken down by country, see Jacob Poushter, *Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies*, PEW RESEARCH CTR. (Feb. 22, 2016), http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies [https://perma.cc/Y3JH-FWPE].

172 Apple, Inc.'s Motion to Vacate Order, *supra* note 52, at 2 ("[O]nce developed for our government, it is only a matter of time before foreign governments demand the same tool.").

173 *Id.*

174 *Governing Intelligence*, *supra* note 64, at 17:40 (statement of Scott Charney, Corporate Vice President, Microsoft Corp.).

175 *Id.* at 17:58 (statement of Scott Charney, Corporate Vice President, Microsoft Corp.).

176 Smith, *supra* note 1, at 13 (emphasis added).

177 *Cybersecurity Tech Accord*, *supra* note 133.

whether criminal or geopolitical" similarly suggests that a user under attack by the U.S. government would receive the same assistance to thwart the intrusion as one under attack by, for example, Russia.[178]

The move among U.S. technology companies to treat the United States as just one among many governments has undoubtedly been an unwelcome development for the U.S. government. As Jon Michaels has documented, in the wake of the September 11 attacks, numerous U.S. companies were willing to provide voluntary informal assistance to the government on intelligence collection,[179] often based on appeals to patriotism.[180] Such techniques are now less effective. Not only has the environment shifted dramatically since the Snowden disclosures, but appeals to patriotism are less effectual when deployed against companies that are trying to denationalize and globalize.

Neutrality essentially means a most (or perhaps least) favored-nation approach to governments: there will be no exceptional treatment for the United States, and companies will only do for the U.S. government that which they are willing to do for all governments. Conversely, if the companies are not willing to do something for any government, they will also not do it for the United States.

The companies' appeal to neutrality does a fair job, whether intentionally or not, of echoing basic international law rights and duties of neutral states.[181] International law on neutrality is part of customary international law, and it is also codified in treaties.[182] Neutrality law does not apply directly to the companies

---

178 *Id.*

179 *See* Michaels, *supra* note 43, at 910-16 (detailing voluntary assistance provided by Western Union and FedEx, among others).

180 *Id.* at 928.

181 Smith's speech invokes the concept of neutrality, but unlike other sections of the speech that reference international treaties, the speech does not specifically mention neutrality law. *See* Smith, *supra* note 1, at 9 (discussing the Fourth Geneva Convention, relating to protection of civilians in armed conflict). The international law of neutrality is not the only extant idea of neutrality. Compare, for example, net neutrality. *See generally* ANGELE A. GILROY, CONG. RESEARCH SERV., R40616, THE NET NEUTRALITY DEBATE: ACCESS TO BROADBAND NETWORKS (2017), https://fas.org/sgp/crs/misc/R40616.pdf [https://perma.cc/9HH3-J6HP] (providing an overview of net neutrality regulatory debates and action). However, it seems to be the one most directly on point for two reasons. First, given that the companies are invoking states as comparators, the international law of neutrality appears to be the most directly analogous, casting states as the prime actors rather than companies, as in the case of net neutrality. Second, the international law of neutrality seems the most likely referent from Smith's speech itself, other portions of which reference the Geneva Conventions, which are foundational treaties on the law of armed conflict. *See* Smith, *supra* note 1, at 9 (discussing the Fourth Geneva Convention). Given this context, understanding references to neutrality to invoke the neutrality applicable in international armed conflict is a small step.

182 *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 553 (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0] (noting that the law of neutrality "is based on Hague Conventions V and XIII and customary international law"); *see also* Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310, 2322-25 [hereinafter Hague Convention V]; Convention Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415, 2427.

because it operates on states and applies during international armed conflict—a circumstance much narrower than the peacetime applicability the companies seek.[183] Nonetheless, the companies' apparent interpretation of the meaning of neutrality both for states and for the companies invokes similar principles.

For countries, neutrality law prohibits states that are parties to an armed conflict from taking certain actions against or on the territory of a neutral state, or using facilities within the neutral state. Most basically, the nationals of states that are not party to the conflict are neutrals,[184] and the territory of a neutral state is "inviolable."[185] In addition, parties to the conflict cannot move "munitions of war or supplies" through neutral territory or erect communications facilities in a neutral state.[186] Brad Smith's call to governments sounds similar. He argues that governments should not take actions that undermine trust in the global information technology infrastructure[187] and that they should "pledge that they will not engage in cyberattacks on the private sector, that they will not target civilian infrastructure."[188] These invocations suggest that the tech companies and their customers should potentially benefit from a double immunity from attack—the immunity afforded to neutrals in an armed conflict and the immunity afforded to civilians.[189]

Neutrality law imposes corresponding obligations on neutral states, and the companies' words and actions echo those obligations too. The companies suggest that as neutral Digital Switzerlands, they will treat all governments equally, giving no government preferential treatment or a free pass to attack users.[190] Similarly, neutrality law requires that if a neutral country takes certain measures to, for example, restrict one warring party's access to communications facilities, it must do the same for all of the warring parties.[191] The companies' emphasis on

183 *See* TALLINN MANUAL 2.0, *supra* note 182, at 553 ("The law of neutrality applies only during international armed conflict.").

184 Hague Convention V art. 16, *supra* note 182, at 2325.

185 *Id.* art. 1 at 2322.

186 *Id.* art. 2 at 2322 ("Belligerents are forbidden to move troops or convoys of either munitions of war or supplies across the territory of a neutral Power."); *id.* art. 3 at 2322 (prohibiting belligerents from, inter alia, erecting military communications facilities in neutral states).

187 *See* Smith, *supra* note 1, at 13-14 ("[W]e need to persuade every government that it needs a national and global IT infrastructure that it can trust. And the only way it can have that is if it knows that our industry is focused on protecting everyone everywhere, and attacking or assisting in attacking no one, anywhere, at any time.").

188 *Id.* at 10.

189 *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 51(2), *opened for signature* Dec. 12, 1977, 1125 U.N.T.S. 3, 26 ("The civilian population as such, as well as individual civilians, shall not be the object of attack."); *see also* Gabriella Blum, *The Dispensable Lives of Soldiers*, 2 J. LEGAL ANALYSIS 115, 117 (2010) ("The foundational principle of distinction . . . grants immunity to civilians.").

190 *See supra* notes 64–68, 177–78 and accompanying text (discussing companies' positions).

191 *See* Hague Convention V art. 8, *supra* note 182, at 2323 ("A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of

playing defense—plugging vulnerabilities and protecting customers from attacks—also sounds in neutrality law. Neutral countries cannot allow violations of their neutrality, and in some circumstances, they have an affirmative obligation to respond to violations of their neutrality.[192] Neutrality in both the traditional context and the new company-centric one can be armed neutrality.[193] In conceptualizing neutrality, the companies are not just calling on states to respect their neutrality, but they appear to be voluntarily assuming obligations akin to those that international law imposes on neutral states.

For all their efforts to appear neutral, however, the companies have not yet achieved—and quite likely will never succeed in achieving—perfect neutrality. They are still strongly associated with the United States, where they remain domiciled and maintain their headquarters. They remain subject to legal process and legal compulsion not just in the United States but in every country where they have assets and operations. This point is key because it ensures that the companies sometimes face a choice between either exiting certain markets or bowing to demands of territorial governments enforcing local laws.[194] Switzerland itself, as a sovereign recognized by other sovereigns, does not face a comparable choice between exit and subordination. In all of these ways, the companies' lack of perfect parity with states not only undermines their claim to parity, but also jeopardizes their ability to be neutral.

Moreover, a posture of neutrality carries with it a risk of undue passivity, tending toward complicity. Switzerland itself fell prey to this risk in World War II. Switzerland's constitution enshrines duties for legislative and executive bodies to safeguard the country's neutrality,[195] but an Independent Commission of Experts, established by the Swiss government to examine Switzerland's actions during World War II, concluded that in various ways Switzerland had

---

wireless telegraphy apparatus belonging to it or to companies or private individuals."); *id.* art. 9 at 2323-24 ("Every measure of restriction or prohibition taken by a neutral Power in regard to the matters referred to in Articles 7 and 8 must be impartially applied by it to both belligerents.").

192 *See id.* art. 5 at 2323 ("A neutral Power must not allow any of the acts referred to in Articles 2 to 4 to occur on its territory. It is not called upon to punish acts in violation of its neutrality unless the said acts have been committed on its own territory.").

193 *Cf.* FED. DEP'T OF FOREIGN AFFAIRS & SWISS FED. COUNCIL, WHITE PAPER ON NEUTRALITY 6 (1993), https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/White_Paper_on_Neutrality.en.pdf [https://perma.cc/SBG5-ACZY] ("Swiss neutrality is armed, which means that Switzerland is determined to avail itself of every means at its disposal to defend itself militarily against any aggressor and to prevent any act incompatible with its neutrality that belligerents may seek to perpetrate on its territory." (emphasis omitted)).

194 *See infra* Section II.C (discussing the limits of the Digital Switzerlands concept, including circumstances in which companies comply with local law).

195 *See* BUNDESVERFASSUNG [BV] [CONSTITUTION] Apr. 18, 1999, SR 101, art. 173, para. 1 (Switz.) (obliging the Federal Assembly to safeguard the country's neutrality); *id.* art. 185, para. 1 (obliging the Federal Council to safeguard the country's neutrality).

compromised its neutrality.[196] For example, while not necessarily technically violating prevailing international law,[197] the conduct of "business as usual" with German banks "enabled Germany . . . to acquire foreign currency which could then be used to obtain essential goods for its war economy."[198]

Embracing a pose of neutrality as a justification for "business as usual"—even if legally permissible—may nonetheless engender justifiable criticism for complicity in governmental action.[199] Social media companies' failure to prevent use of their platforms by agents of the Russian government in the 2016 election cycle falls in this category.[200]

Although the companies' analogy to neutrality law is imperfect, it remains intriguing and may provide a principled platform for engagement with governments going forward, as well as a cautionary tale to avoid complicity in governmental conduct.

C. *The Scope and Limits of Digital Switzerlands*

Focusing on the companies' shift from cooperation with to sometimes countering governments pursuant to the Digital Switzerlands mantle is not meant to suggest that they are models of virtue or unflinching defenders of human rights. The fact that they are countering governments, especially the U.S. government, at all in the claimed service of protecting users is notable, new, and worth considering. But it is also limited.

---

196 The most reprehensible violations involved treatment of refugees. *See* INDEP. COMM'N OF EXPERTS SWITZ.—SECOND WORLD WAR, SWITZERLAND, NATIONAL SOCIALISM AND THE SECOND WORLD WAR: FINAL REPORT 499 (2002), https://www.uek.ch/en/schlussbericht/synthesis/ueke.pdf [https://perma.cc/7V4H-RE22] ("[M]easured against its previous stand in terms of humanitarian aid and asylum where its refugee policy was concerned, neutral Switzerland not only failed to live up to its own standards, but also violated fundamental humanitarian principles.").

197 *See id.* at 252 (explaining that although the transactions were defended on the ground "that the gold purchases were required as a result of Switzerland's neutrality," "this is as unconvincing an argument as the opposite view, often put forward by the Allies, that the purchases violated Switzerland's neutrality," because "[i]n fact, neutrality neither prohibited nor required such purchases: it merely permitted them"). Switzerland also purchased gold from the Allies, but as the Report notes, such purchases were "not directly comparable to the purchases from Germany since the Allied gold constituted a lawfully acquired means of payment and currency reserves." *Id.* at 242.

198 *Id.* at 247 (emphasis omitted).

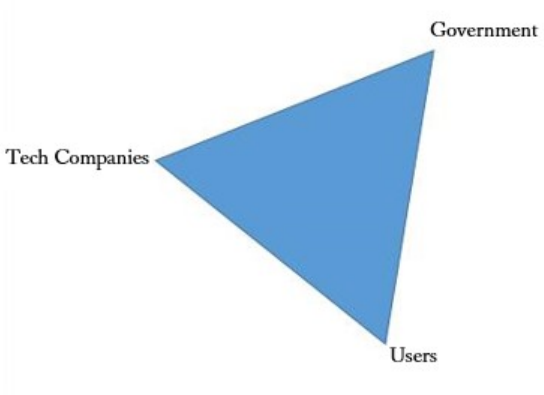
199 *Cf.* Adam J. White, *Google.gov*, NEW ATLANTIS, Spring 2018, at 3, 7-8 (noting, with respect to Google's alleged "neutrality" as a search engine, that "[t]he standard of neutrality is itself not value-neutral but a moral standard of its own, suggesting a deeper ethos and aspiration about information"); *infra* notes 211–14 (discussing the risks of operating in nondemocratic states).

200 *Cf. Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before the U.S. Senate Comm. on the Judiciary & the U.S. Senate Comm. on Commerce, Sci. & Transp.*, 115th Cong. (2018), https://www.judiciary.senate.gov/imo/media/doc/04-10-18%20Zuckerberg%20Testimony.pdf [https://perma.cc/Q7ZW-LDRH] (statement of Mark Zuckerberg, Chairman & Chief Executive Officer, Facebook, Inc.) ("There's no question that we should have spotted Russian interference earlier . . . .").

Importantly, the Digital Switzerlands concept does not directly address the many concerns stemming from the role of the technology companies as what Julie Cohen has called "surveillance principals in their own right,"[201] amassers and exploiters of vast quantities of user-created data. And even as to the government relationships about which the Digital Switzerland idea is primarily concerned, the companies are not challenging governments all the time, only some of the time, and they fall short of ideal levels of protection for individuals. The companies are strategic in when they launch challenges, including by doing so only when they have viable legal arguments. Exploring the scope of the Digital Switzerlands idea—when it applies and when it doesn't—helps to clarify when and why companies attempt to counter governments and when and why they don't.

The companies are challenging governments in a generally coherent and predictable pattern. The pattern of company challenges becomes clear when the cyberspace ecosystem is understood as a triangle, composed of three separate power centers: governments, technology companies, and users, as illustrated in Figure 1 below.[202]

Figure 1: Triangulating When Tech Companies Fight and Fold



201 Cohen, *supra* note 18, at 194; *see also supra* note 6 and accompanying text (discussing the many concerning issues surrounding the companies' relationship to users, including, for example, exploitation of user data).

202 Others have suggested similar triadic framings in the service of other types of arguments. *See* Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1187-88 (2018) (describing a pluralist model of free speech regulation that involves "at least three different groups": "the state and supra-national entities like the European Union," "companies that operate the digital infrastructure, especially search engines and social media platforms," and "speakers who use the digital infrastructure to communicate"); Birnhack & Elkin-Koren, *supra* note 20, at ¶¶ 122-30 (arguing for a triangular relationship of governments, online service providers (OSPs), and citizens to illustrate the insufficiency of U.S. constitutional law in remedying privacy harms caused by OSPs' collaboration with governments).

This model, like all models, is necessarily a simplification.[203] It reduces a complex ecosystem to a few discrete points to isolate factors with explanatory power. No point on the triangle—governments, companies, or users—is monolithic,[204] and instances where there are divergent interests within, for example, users pose complications for the model, as discussed below.[205] Nonetheless, the triangular framing is *less* simplified than the frequent focus on only two points of the triangle—governments' relationship to users, governments' relationship to companies, or companies' relationship to users.[206] The triangular framing complicates these narratives by positing the importance of alliances between power centers against other power centers.

The triangular framing helps to illustrate when companies, if they take seriously the Digital Switzerlands idea, should fight against governments, and when they are likely to "fold" and comply without resisting. Stated generally, the Digital Switzerlands concept suggests that companies will fight against or resist governments when the companies perceive themselves to be and can credibly argue that they are protecting the interests of users against governments, as illustrated in Figure 2.[207] In the parlance of neutrality law, a company's users are akin to a state's citizens, and thus attacks on the user citizens are violations of neutrality.[208] The companies determine users' interests for themselves, and due to limited information or skewed

---

203 For example, the model does not explicitly address the role of international institutions, like the United Nations, or of multistakeholder organizations, like the Internet Corporation for Assigned Names and Numbers (ICANN) or the Internet Engineering Task Force, except to the extent that they are a type of "user." It also does not address the role of Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs). *See, e.g.*, *CERT-EU*, EUR. UNION AGENCY FOR NETWORK & INFO. SEC., https://www.enisa.europa.eu/topics/csirts-in-europe/capacity-building/european-initiatives/cert-eu [https://perma.cc/SV7Y-KFDA] (last visited Feb. 8, 2019). These entities might plausibly argue that they are more neutral and Switzerland-like than tech companies. But some of them do not deal with the security issues that this Article primarily addresses, and others, particularly multistakeholder entities, have cross cutting memberships that incorporate representatives from all points on the triangle. The model's omission of these entities is not meant to downplay their importance on many cyberspace-related issues; rather, it is simply an effort to isolate a set of relationships between tech companies, users, and governments that are exerting exceptionally strong influence in particular circumstances, as discussed in the remainder of this Section.

204 *See, e.g.*, WOODS, *supra* note 18, at 2 (noting differences in willingness to challenge states between hardware and data services firms and "consumer-facing" versus enterprise companies); *Developments in the Law—More Data, More Problems*, *supra* note 60, at 1741 (discussing technology companies as "surveillance intermediaries" and noting that they "are not a monolith," but rather have "different user bases, business models, income streams, and public relations strategies").

205 *See infra* notes 216–18.

206 *See, e.g.*, GOLDSMITH & WU, *supra* note 12 (focusing on governments' power to regulate individuals); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016) (focusing on companies' relationships to users); Rahman, *supra* note 2 (same).

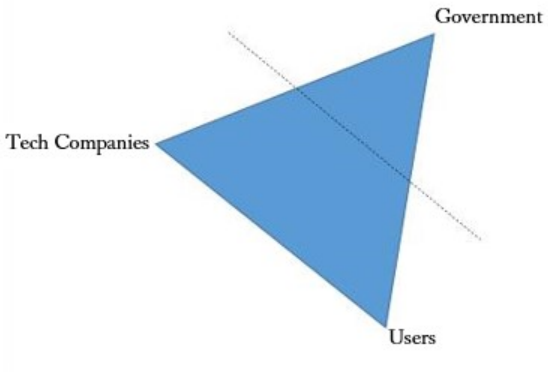
207 For an explanation of the motivations for this behavior, see *supra* Sections II.A–B.

208 *See supra* notes 186–93 and accompanying text (discussing neutrality law).

perceptions, they may not always be correct in their assessments, sometimes fighting when they shouldn't and failing to fight when they should.

Paradigmatic easy cases where companies perceive an alignment with users against governments—and where the model therefore provides clear guidance for the companies—involve the preservation of technical security measures, as in the Apple/FBI case, and the lawsuits that companies have filed in order to disclose government access to user content. In the latter cases, the companies are claiming the mantle of user protection through transparency and disclosure.

Figure 2: When Companies Fight



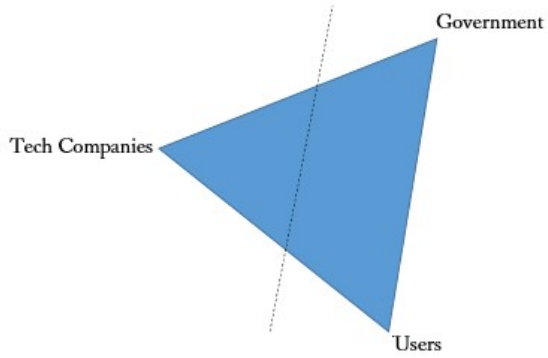
The triangular framing also suggests important contexts in which the companies will *not* fight governments. In particular, companies are most likely to "fold" when, based on the companies' assessment, there is an alliance between users and governments, as illustrated in Figure 3. This category includes many routine cases. For example, technology companies regularly comply with requests to take down content in a variety of circumstances, including government requests to take down content that violates local laws.[209] The companies also routinely comply when served with legal process requiring them to produce the contents of user accounts.[210]

---

209 *See, e.g.*, *Government Requests to Remove Content*, GOOGLE, https://transparencyreport.google.com/government-removals/overview [https://perma.cc/478K-BBYW] (last visited Feb. 8, 2019) (explaining that governments request content removals for, inter alia, violation of local law, and providing statistics on the frequency and outcomes of such requests).

210 *See, e.g.*, *Legal Process for User Data Requests FAQs*, GOOGLE, https://support.google.com/transparencyreport/answer/7381738 [https://perma.cc/6MKA-HTW4] (last visited Feb. 8, 2019) (explaining that the U.S. "government needs legal process—such as a subpoena, court order or search warrant—to force Google to disclose user information"); *Requests for User Information*, GOOGLE, https://transparencyreport.google.com/user-data/overview [https://perma.cc/NG4Y-WP5W] (last visited Feb. 8, 2019) (reporting that from July 1, 2016 through January 1, 2017, roughly sixty-five percent of

Figure 3: When Companies Fold



One way companies appear to understand the existence of an alliance between governments and users is government compliance with and attempts to enforce democratically enacted laws. For example, countries around the world have different understandings of the scope of free expression rights. Even among Western democracies, there is longstanding and significant disagreement over, for example, whether and how to regulate hate speech. The companies deal with these variations by complying with local law in the countries in which they operate, which means the scope of content subject to government takedown requests for violating local law is considerably different in the United States as compared to, for example, many European countries. Nonetheless, the democratically determined scope of free expression in each country is a matter established through the interaction of users and governments, and why then should a U.S. company challenge those determinations on the basis of broader U.S. understandings of free expression? The companies generally don't. Companies will "fold"—complying with, rather than challenging, government requests—when they perceive governments and users to be aligned.

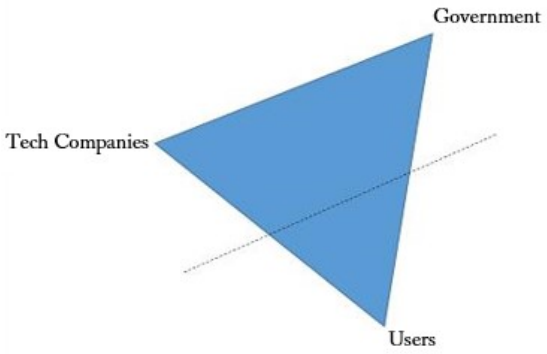
The examples already discussed are the comparatively easy ones. Various complications make it more difficult for companies to assess where the interests of users lie and therefore how to apply the Digital Switzerlands idea.

One complication arises when the government involved is not democratic. Then the assumption that local law represents an alliance between users and the government—as opposed to oppression of users by the government—is less tenable or perhaps entirely untenable. This may manifest in government requests to take down content critical of the government, or, in a recent

requests for data resulted in production of some data); *see also* Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 236-37 (2018) (noting that U.S. tech companies "produce data in response to approximately fifty to seventy-five percent of" government requests for information).

example, Chinese government demands to remove Virtual Private Network (VPN) apps that allow for secure, uncensored communications.[211] Critics allege that in those circumstances, the companies are not allied with users, but rather are complicit in government repression of users, as illustrated in Figure 4.[212] Companies in this circumstance may confront a choice between exiting a country or facing charges of complicity.

Figure 4: The Alliance to Be Avoided



Another related complication is that companies claiming to act for the benefit of users may misunderstand, misrepresent, or project their own misperception of users' interests. "Users" are not monolithic and frequently have divergent interests. And companies do not ascertain user interests through processes of democratic governance.[213] The China VPN example illustrates this difficulty. In defending their decision to bow to this and other government demands, companies have argued that it is better for users if the companies stay in the market, rather than pulling out altogether.[214] In other words, the companies argue

211 *See, e.g.*, Emily Rauhala, *Apple, Amazon Help China Curb the Use of Anti-Censorship Tools*, WASH. POST (Aug. 2, 2017), https://www.washingtonpost.com/world/asia_pacific/holes-close-in-chinas-great-firewall-as-apple-amazon-snub-apps-to-bypass-censors/2017/08/02/77750f38-7766-11e7-803f-a6c989606ac7_story.html [https://perma.cc/6Q26-X3HA] (reporting steps by Apple and Amazon to prevent consumer access to VPN apps at the request of the Chinese government).

212 *See, e.g.*, Amul Kalia & Eva Galperin, *Deciphering China's VPN Ban*, ELEC. FRONTIER FOUND. (Aug. 2, 2017), https://www.eff.org/deeplinks/2017/08/deciphering-chinas-vpn-ban [https://perma.cc/R7Y8-ZRUR] (arguing that by removing the VPN apps from its app store, Apple "has once again aided the Chinese government in its censorship campaign against its own citizens").

213 *See infra* Section III.B.

214 *See* Rauhala, *supra* note 211 (quoting Apple CEO Tim Cook explaining that pulling the VPN apps was preferable to Apple exiting the Chinese market because "participating in markets and bringing benefits to customers is in the best interest of the folks there and in other countries, as well"). If Google reenters China with a censored search app, it may justify the decision with similar arguments. *See* Farhad Manjoo, *Google Tried to Change China. China May End Up Changing Google.*, N.Y. TIMES (Aug. 22, 2018), https://www.nytimes.com/2018/08/22/technology/google-

that folding in the face of government demands for content censorship in nondemocratic states is more like Figure 2 than Figure 4, because it allows them to serve users by remaining in the censoring country and increasing users' access to information, at least to some extent.[215] This defense is highly debatable. It could simultaneously be criticized as a convenient rationalization and defended as a reasonable judgment in the face of a difficult tradeoff.

Another complication for the companies attempting to protect users against governments arises when local law has extraterritorial effects. Although the companies generally seem to understand users and governments to be allied when democratically enacted laws are applied, extraterritorial effects of local law cause a problem because they pit the interests of subsets of the companies' users against one another. One example of this phenomenon involves the "right to be forgotten" in European law. U.S. technology companies have established routine processes to implement requests for delisting of search results pursuant to the right to be forgotten.[216] But Google is currently litigating a challenge to an order from the French data protection authority that requires Google to delist search results across all Google domains (including google.com) regardless of where in the world the user attempting to search for the link is located.[217] The expansive French order pits the rights of Google users in Europe to exercise their right to be forgotten against the rights of Google users elsewhere to freely access information. In the face of competing user interests, Google has chosen to

china-conventionality.html (reporting that Google CEO Sundar Pichai made such arguments in a meeting with employees); McKune & Deibert, *supra* note 33 (discussing the rationales for and circumstances of Google's possible reentry). *But see supra* note 33 (noting that Google appears to have halted the project for now).

215 *Cf.* MACKINNON, *supra* note 18, at 138 (noting that "China's liberal bloggers . . . tended to support the decision by Microsoft and Google to provide service to Chinese users," despite the fact that the services were censored); *id.* at 174 ("Blocking US Internet and telecommunications companies from ever operating in authoritarian or quasi-democratic countries amounts to counterproductive overkill, preventing citizens from using some of the world's most innovative and open technology to advocate for change . . . .").

216 *See, e.g.*, *EU Privacy Removal*, GOOGLE, https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf [https://perma.cc/FWX4-ZMY7]; *Request to Block Bing Search Results in Europe*, BING, https://www.bing.com/webmaster/tools/eu-privacy-request [https://perma.cc/D79K-TZA5].

217 *See* Kent Walker, *A Principle That Should Not Be Forgotten*, GOOGLE: THE KEYWORD (May 19, 2016), https://www.blog.google/topics/google-europe/a-principle-that-should-not-be-forgotten [https://perma.cc/3YDA-92P5] (discussing the French order and Google's response). This would be an expansion of Google's current practice, which involves delisting search results from "all European versions of Google Search," as well as "us[ing] geolocation signals (like IP addresses) to restrict access to the delisted URL on all Google Search domains, including google.com, when accessed from the country of the person requesting the removal." Peter Fleischer, *Adapting Our Approach to the European Right to Be Forgotten*, GOOGLE: THE KEYWORD (Mar. 4, 2016), https://www.blog.google/topics/google-europe/adapting-our-approach-to-european-rig [https://perma.cc/BH8T-WCE6].

fight the French order, and the challenge is pending before the European Court of Justice (ECJ).[218]

As all of these examples indicate, technology companies face difficult dilemmas with respect to government requests or demands that the companies impose content controls.[219] When the content controls result from local law in democratic countries, the triangular framing explains why companies often do not challenge the orders. The model also suggests, however, circumstances when the companies might fight government orders, especially when purportedly local law infringes on the rights of users outside the ordering country. Companies have also dealt with concerns about government-requested content controls by establishing a practice of releasing extensive transparency reports that detail requests for content removal, including the government agency, court order, or other removal requester and the nature of information removed.[220]

Yet another complication has recently emerged. To determine whether to fight or to cooperate with governments, companies must first perceive that government action is occurring. That task can sometimes be complicated, as shown by the multitude of revelations about Russian use of social media to influence the 2016 U.S. election.[221] U.S. tech companies were caught flat footed. Before and during the election cycle, they suffered from similar failures of imagination to those that plagued U.S. government actors and commentators. And even as Russian actors made significant use of platforms like Facebook and Twitter, the companies failed to appreciate what was happening, much less to

---

218 *See, e.g.*, Alex Hern, *ECJ to Rule on Whether "Right to Be Forgotten" Can Stretch Beyond EU*, GUARDIAN (UK) (July 20, 2017, 5:19 EDT), https://www.theguardian.com/technology/2017/jul/20/ecj-ruling-google-right-to-be-forgotten-beyond-eu-france-data-removed [https://perma.cc/JY3A-VME3] (noting that the case asks the ECJ to clarify the scope of its 2014 ruling on the right to be forgotten).

219 In addition to the risk of the companies being coopted by governments, there is also a risk of the reverse occurring: companies coopting governments in ways that harm users. For example, Facebook's Free Basics service, which provides limited Internet access to sites curated by Facebook for free in less developed countries, has been criticized as "digital colonialism." Olivia Solon, *'It's Digital Colonialism': How Facebook's Free Internet Service Has Failed Its Users*, GUARDIAN (July 27, 2017, 8:00 EDT), https://www.theguardian.com/technology/2017/jul/27/facebook-free-basics-developing-markets [https://perma.cc/ST3K-XD9V] (quoting Ellery Biddle, Global Voices). For an in-depth discussion of the backlash and ultimate government regulation that blocked Free Basics in India, see Rahul Bhatia, *The Inside Story of Facebook's Biggest Setback*, GUARDIAN (May 12, 2016, 1:00 EDT), https://www.theguardian.com/technology/2016/may/12/facebook-free-basics-india-zuckerberg [https://perma.cc/7J2J-27F6].

220 *See, e.g.*, *Facebook Transparency Report*, FACEBOOK, https://transparency.facebook.com [https://perma.cc/S7PB-UE8U] (last visited Feb. 8, 2019); *Government Requests to Remove Content*, *supra* note 209; *Removal Requests*, TWITTER, https://transparency.twitter.com/en/removal-requests.html [https://perma.cc/7E2N-ZYST] (last visited Feb. 8, 2019); *Search Removals Under European Privacy Law*, GOOGLE, https://transparencyreport.google.com/eu-privacy/overview [https://perma.cc/5EF2-SWYT?type=image] (last visited Feb. 8, 2019).

221 *See* Streitfeld, *supra* note 2 (noting with respect to Russian election interference that "[t]he manipulation was so efficient and so lacking in transparency that the companies themselves barely noticed it was happening").

react effectively.[222] As Facebook eventually admitted, "In the run-up to the 2016 elections, we were focused on the kinds of cybersecurity attacks typically used by nation states, for example phishing and malware attacks. And we were too slow to spot this type of information operations interference."[223]

This lack of understanding is a practical complication more than a theoretical one. With the benefit of current information, the application of the triangle framing suggests a path forward for the companies. The actions of the Russian government in attempting to spread misinformation and exacerbate social tensions are clearly at odds with the interests of U.S. users in legitimate debate and a fair electoral process. Thus, per the Digital Switzerlands model, the companies should act to protect U.S. users from the Russian government's actions and from similar governmental actions going forward. With varying degrees of reluctance, the companies have begun to do

222 *See* Adam Entous, Elizabeth Dwoskin & Craig Timberg, *Obama Tried to Give Zuckerberg a Wake-Up Call over Fake News on Facebook*, WASH. POST (Sept. 24, 2017), https://www.washingtonpost.com/business/economy/obama-tried-to-give-zuckerberg-a-wake-up-call-over-fake-news-on-facebook/2017/09/24/15d19b12-ddac-4ad5-ac6e-ef909e1c1284_story.html [https://perma.cc/CQE7-HK4Y] (reporting that in November 2016, President Obama "made a personal appeal to Zuckerberg to take the threat of fake news and political disinformation seriously," and that "[l]ike the U.S. government, Facebook didn't foresee the wave of disinformation that was coming and the political pressure that followed"). Company representatives have admitted as much in recent congressional testimony. *See Social Media Influence in the 2016 U.S. Election: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. 18 (2017) [hereinafter *Election Hearings*] (statement of Sean J. Edgett, Acting Gen. Counsel, Twitter, Inc.) ("Twitter is familiar with problems of spam and automation, including how they can be used to amplify messages. The abuse of those methods by sophisticated foreign actors to attempt state-sponsored manipulation of elections is a new challenge for us—and one that we are determined to meet."); *id.* at 12 (statement of Colin Stretch, Gen. Counsel, Facebook) ("After the 2016 election, we learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the election by exploiting Facebook's ad tools. This is not something we had seen before, and so we started an investigation that continues to this day.").

223 *Russian Ads Released by Congress*, FACEBOOK: NEWSROOM (May 10, 2018), https://newsroom.fb.com/news/2018/05/russian-ads-released-by-congress/?wpisrc=nl_cybersecurity202&wpmm=1 [https://perma.cc/GW43-33MM].

so, under sustained pressure from the U.S. Congress,[224] and the efficacy of their efforts remains open to debate.[225]

For all these reasons, the Digital Switzerland idea is limited in scope. It is not a promise by the companies to fight governments in all circumstances or every instance where human rights advocates would wish. Rather, from the companies' perspective(s), the Digital Switzerland framing suggests they should resist governments where they can raise plausible legal arguments and credibly claim to be allied with users when the interests of users and government diverge. This account explains why the companies have challenged government actions that threaten technical security and why they have sought transparency related to government access to user account content. Circumstances where the interests of users are set against one another and where, for various reasons, there is a serious question about whether compliance with local law serves user interests raise difficult questions for the companies, which sometimes fight and sometimes fold. The Digital Switzerlands model is idealized both in its simplification of the cyberspace ecosystem and in its description of the companies' behavior. The companies' actual instantiation of the Digital Switzerlands concept remains flawed, as the Russian election interference response shows. But flaws in implementation may be remedied over time, and even now, they do not

224 Executives have given overviews of their companies' responses in testimony to Congress. *See Election Hearings*, *supra* note 222, at 22-33 (statement of Sean J. Edgett, Acting Gen. Counsel, Twitter, Inc.) (discussing Twitter's response); *id.* at 11-15 (statement of Colin Stretch, Gen. Counsel, Facebook) (discussing Facebook's response); *id.* at 43-44 (statement of Kent Walker, Senior Vice President & Gen. Counsel, Google) (discussing Google's response); *see also Russian Ads Released by Congress*, *supra* note 223 (detailing measures about, for example, ad transparency and disabling accounts run by Russia's Internet Research Agency). Of course, the risk of foreign government interference is not limited to the United States. The companies' duty to protect users from such interference extends to all countries where their users are at risk of manipulation, and they have begun to take actions to address manipulation concerns worldwide. *See, e.g.*, Nathaniel Gleicher, *Taking Down More Coordinated Inauthentic Behavior: What We've Found So Far*, FACEBOOK: NEWSROOM (Aug. 21, 2018), https://newsroom.fb.com/news/2018/08/more-coordinated-inauthentic-behavior [https://perma.cc/969B-ZCMH] (reporting on Facebook's removal of accounts linked to Russian military intelligence and Iranian state media "for coordinated inauthentic behavior" targeted at people in "the Middle East, Latin America, UK and US").

225 Legislators are considering taking the companies' response out of the realm of voluntary action and regulating at least some actions, particularly foreign-linked ad purchases. *See* Cecelia Kang, Nicholas Fandos & Mike Isaac, *Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill*, N.Y. TIMES (Oct. 31, 2017), https://www.nytimes.com/2017/10/31/us/politics/facebook-twitter-google-hearings-congress.html (reporting support among Democratic and Republican Senators for regulating political ad funding). The Honest Ads Act, S. 1989, 115th Cong. (2017), would impose disclosure requirements for political ad purchases on online platforms. With Senator John McCain's death, the bill lost its sole Republican cosponsor. Nonetheless, because this bill involves the U.S. government protecting U.S. users from foreign government meddling, the Digital Switzerlands framing suggests that the companies should not oppose it, and indeed some companies have announced their support. *See infra* notes 296–301 and accompanying text (discussing the Honest Ads Act and noting that some companies, including Microsoft and Facebook, have announced support for the bill).

decrease the importance of the normatively laden questions that the companies' Digital Switzerlands self-conception raises.

The remaining Part of this Article takes up these issues.

III. IMPLICATIONS OF THE RISE OF DIGITAL SWITZERLANDS

The existence and continued growth of U.S. technology companies will have a number of implications. This Part identifies some of the most salient impacts and provides tentative thoughts on the extent to which the rise of technology companies as Digital Switzerlands is beneficial or detrimental.

A. *Individuals' Power and Freedom*

Consider first the overall power of individuals. On the one hand, the companies represent a new and additional layer of power over individuals. In very real ways, they regulate users—how users access information, whether communications are secure, the extent to which users' privacy is protected, etc. As Larry Lessig has explained, "[t]he software and hardware that make cyberspace what it is constitute a set of constraints on how you can behave," and while "[t]he substance of these constraints may vary, . . . they are experienced as conditions on your access to cyberspace."[226] Code, including code written by technology companies, constitutes regulation.[227] It "embeds certain values or makes certain values impossible."[228] Technology companies have been regulators for as long as they have written code. But the relative importance of their role as regulators has accelerated with the ever-increasing dependence of users on the hardware and software that they create and sell.

While technology companies are an added layer of regulation and regulators over individuals, their rise also represents a relative decline in governmental power over users. As discussed above, the companies have become, in certain circumstances, powerful forces standing between governments and individuals or with individuals against governments.[229] Companies have defended users against claims to government data access in several recent cases,[230] and they have filed lawsuits against the government to

---

226 LAWRENCE LESSIG, CODE 124 (2d ed. 2006); *see also* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 555-56 (1998) (arguing that "the set of rules for information flows imposed by technology and communication networks form a 'Lex Informatica'" that regulates users).

227 LESSIG, *supra* note 226, at 125. For an overview of the literature addressing regulation by code and its challenges, see Mulligan & Bamberger, *supra* note 138, at 711-22.

228 LESSIG, *supra* note 226, at 125.

229 *Cf. supra* notes 211–12 and accompanying text (discussing the challenges posed by nondemocratic states).

230 *See supra* notes 51–58 and accompanying text; *see also* Dan Levine & Joe Menn, *Exclusive: U.S. Government Seeks Facebook Help to Wiretap Messenger - Sources*, REUTERS (Aug. 17, 2018, 4:34 PM),

empower individuals by providing them with more information about government demands for information.[231]

Sometimes, the technology companies are the only parties in a position realistically to challenge government demands. The companies are on notice about government demands in a way that individual users often are not.[232] The companies are the recipients of the government requests for information or modification of technology, whereas individual users often have no idea their information has been the subject of a request, sometimes precisely because of gag orders imposed on the companies. Moreover, as the recipients of government demands and court orders, the companies clearly have standing to challenge government actions.[233] Standing has been a persistent problem for potential suits by users. In some cases, users have difficulty satisfying standing requirements because they cannot show that they personally have been targeted or will have their security compromised in the future, and therefore cannot meet the requirements for an injury in fact.[234] In other cases, courts have not deemed government intrusions on individual privacy interests legally cognizable.[235]

Even if technology companies are not the only possible challengers, their other advantages make them *effective* challengers. They are extremely well resourced and capable of hiring top-notch legal counsel to bring and defend cases.[236] They are also

---

https://www.reuters.com/article/us-facebook-encryption-exclusive/exclusive-u-s-government-seeks-facebook-help-to-wiretap-messenger-sources-idUSKBN1L226D [https://perma.cc/X82L-ASNP] (reporting that Facebook is resisting in court a government demand to write code to allow law enforcement to eavesdrop on a suspect's voice conversations in Facebook Messenger); Ellen Nakashima, *Facebook Wins Court Battle over Law Enforcement Access to Encrypted Phone Calls*, WASH. POST (Sept. 28, 2018), https://www.washingtonpost.com/world/national-security/facebook-wins-court-battle-over-law-enforcement-access-to-encrypted-phone-calls/2018/09/28/df438a6a-c33a-11e8-b338-a3289f6cb742_story.html [https://perma.cc/XL37-5JAJ] (reporting that a federal judge "ruled that the government cannot force Facebook to break the encryption on its popular Messenger voice app").

231 *See supra* notes 60–63 and accompanying text.

232 *See* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 157 (2018) (noting that "surveillance intermediaries" can overcome the standing problems that hinder individual plaintiffs because they "know whenever a program is used" and thereby also have "the flexibility to choose the best litigating posture").

233 *See, e.g.*, *Developments in the Law—More Data, More Problems*, *supra* note 60, at 1739 (highlighting the doctrinal and practical advantages the tech companies have over individuals seeking to challenge government surveillance). *But see* Jennifer Daskal, *Notice and Standing in the Fourth Amendment: Searches of Personal Data*, 26 WM. & MARY BILL RTS. J. 437, 444-47 (2017) (discussing cases in which judges took a restrictive view of company standing for Fourth Amendment claims).

234 *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) (discussing requirements for Article III standing).

235 This may be changing. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (limiting the Fourth Amendment third-party doctrine).

236 *See, e.g.*, Taylor Goldenstein, *High-Profile Attorney Ted Olson Joins Apple's Fight Against FBI Terror Probe*, L.A. TIMES (Feb. 18, 2016, 12:03 PM), http://www.latimes.com/local/lanow/la-me-ln-ted-olson-joins-apple-fight-against-fbi-20160218-story.html [https://perma.cc/F54H-W7V4] (discussing Apple's representation by former Solicitor General Ted Olson); *see also* Rozenshtein, *supra* note 232, at 157 (noting that companies "have the resources to litigate frequently and to the bitter end").

sophisticated organizations that have personnel dedicated to public relations, and they have embraced the public sphere, not just the courts, as a battleground in pushing back against government requests.[237] The companies' sophistication has also manifested in their ability and willingness to coordinate support for whichever company takes the lead on a particular issue. They have joined suits brought by other companies, filed joint amicus briefs, and issued supportive public statements.[238] Market-based interests, stemming from the companies' global reach, can incentivize them to deploy their considerable resources in support of security-based concerns affecting users, as discussed above.[239]

While not dismissing the potentially negative impact on individuals from having an added layer of regulation, for now, the actions of technology companies as Digital Switzerlands often appear to have a positive effect on the power of individual users vis-à-vis governments. The companies have proven to be effective challengers to the exercise of certain types of government power over individuals, namely government claims related to access to and the security of user account content.

The idea that the existence of two regulators can sometimes produce gains for individual freedom is not a new one. In *The Federalist No. 51*, James Madison addressed the U.S. federal system and argued that because of the dual federal and state sovereigns, "a double security arises to the rights of the people."[240] The Supreme Court has echoed this idea, with Justice Kennedy explaining in a recent majority opinion: "The federal system rests on what might at first seem a counterintuitive insight, that 'freedom is enhanced by the creation of two governments, not one.'"[241] The reason that two governments are understood to be paradoxically more protective is because,

237 For an example, see Apple CEO Tim Cook's statement to Apple customers regarding Apple's decision to fight the court order in the San Bernardino case. Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter [https://perma.cc/S4UF-B8J4].

238 For discussion and a visual representation of the support networks among the tech companies, see Dina Bass & David Ingold, *The Top Five Tech Rivals Join Forces to Shape Policy—And Fight the Government*, BLOOMBERG (June 27, 2017, 4:00 AM EDT), https://www.bloomberg.com/news/features/2017-06-27/the-top-five-tech-rivals-join-forces-to-shape-policy-and-fight-the-government. *See, e.g.*, Brief for Technology Companies as *Amici Curiae* in Support of Respondent at 2-7, United States v. Microsoft Corp., No. 17-0002 (U.S. Jan. 18, 2018), 2018 WL 557075, at *2-6 (showing amicus support for Microsoft from technology companies, including Amazon, Apple, Facebook, and Google).

239 *See supra* Section II.A. The stability of these incentives is a separate question taken up later in this Part. *See infra* Section III.D.

240 THE FEDERALIST NO. 51, at 323 (James Madison) (Clinton Rossiter ed., 1961).

241 Bond v. United States, 564 U.S. 211, 220-21 (2011) (quoting Alden v. Maine, 527 U.S. 706, 758 (1999)); *see also* New York v. United States, 505 U.S. 144, 181 (1992) ("[T]he Constitution divides authority between federal and state governments for the protection of individuals. State sovereignty is not just an end in itself: 'Rather, federalism secures to citizens the liberties that derive from the diffusion of sovereign power.'" (quoting Coleman v. Thompson, 501 U.S. 722, 759 (1991) (Blackmun, J., dissenting))); Gregory v. Ashcroft, 501 U.S. 452, 459 (1991) ("In the tension between federal and state power lies the promise of liberty.").

as Madison argued, "[t]he different governments will control each other," checking their respective powers for the benefit of the people.[242] Madison's basic insight remains applicable in the company-versus-government context: having two powerful regulators, rather than only one, can sometimes strengthen individuals' freedom, liberty, and security because often it takes a powerful regulator to challenge and check another powerful regulator.

However, the quasi-sovereign status of U.S. technology companies does not make for a perfect analogy to U.S. states or to the U.S. federal system because one of the regulators is not democratic. The companies' democracy deficit raises concerns addressed in the next Section.

B. *Democracy and Accountability*

Another significant concern with technology companies taking on a role akin to sovereigns is that they are undemocratic. The legitimacy of governments is often judged by the extent to which they are "democratic." While the meaning and essential characteristics of a democracy are contested,[243] a common feature is voting and elections as a means of ensuring government responsiveness to and representativeness of citizens.[244]

With elections as a metric of democracy, the technology companies do not fare well. At least for users who are not also shareholders, the companies don't hold votes. Users don't elect company leaders or vote on policy changes. Changes to Facebook's privacy policy, for example, are imposed, not voted into effect.[245] Users are given notice, but not a choice.[246] Similarly, when Apple chose to resist the U.S.

---

242 THE FEDERALIST NO. 51, *supra* note 240, at 323.

243 *See, e.g.*, ROBERT A. DAHL, DEMOCRACY AND ITS CRITICS 2 (1989) (arguing that "democracy . . . nowadays is not so much a term of restricted and specific meaning as a vague endorsement of a popular idea"); Erwin Chemerinsky, *Foreword: The Vanishing Constitution*, 103 HARV. L. REV. 43, 71 (1989) ("Political science theorists disagree greatly about what 'democracy' means, and no one theory can claim axiomatic status.").

244 *See, e.g.*, ROBERT A. DAHL, DILEMMAS OF PLURALIST DEMOCRACY 10-11 (1982) (defining democracy based on seven characteristics, including elections); Samuel Issacharoff, *Fragile Democracies*, 120 HARV. L. REV. 1405, 1411 (2007) ("When stripped down to their essentials, all definitions of democracy rest ultimately on the primacy of electoral choice and the presumptive claim of the majority to rule.").

245 Facebook did experiment with a version of direct democracy in 2009. *See Facebook Opens Governance of Service and Policy Process to Users*, FACEBOOK: NEWSROOM (Feb. 26, 2009), https://newsroom.fb.com/news/2009/02/facebook-opens-governance-of-service-and-policy-process-to-users [https://perma.cc/35LA-3AKQ] (announcing mechanisms for voting on several policies). The experiment was short-lived. *See* Adi Robertson, *Mark Zuckerberg Wants to Democratize Facebook—Here's What Happened When He Tried*, VERGE (Apr. 5, 2018, 1:40 PM EDT), https://www.theverge.com/2018/4/5/17176834/mark-zuckerberg-facebook-democracy-governance-vote-failure [https://perma.cc/TDH4-WBBM] (discussing low voting rates and Facebook's abandonment of the voting process).

246 This is not to imply that users have no "voice" options, but simply that elections—the quintessential voice option in democratic governments—are not available. *See* ALBERT O. HIRSCHMAN, EXIT, VOICE, AND LOYALTY: RESPONSES TO DECLINE IN FIRMS,

government's requests for assistance in accessing the San Bernardino shooter's iPhone, it did not hold a vote among Apple users.

The lack of enfranchisement among the companies' users as to companies' policy choices masks, however, a type of enfranchisement that the companies' users do possess. Corporate "citizenship" is voluntary. Individuals choose to become part of a company's user base and to associate themselves with the company, for whatever protection it may or may not provide. Unlike national citizenship, corporate allegiance isn't assigned by birth.

Not only do users have a choice in associating themselves with particular companies, they also have a choice in *disassociating*. In other words, users can vote with their feet, dollars, and service choices, exercising exit rights.[247] The exit rights accompanying corporate "citizenship" are fairly easy—though not totally painless—to exercise.[248] Users can exchange one corporate allegiance for another or acquire multiple corporate allegiances much more easily than they can with respect to citizenships in territorial states.[249]

Lessig describes the distinction as one between "citizen-sovereignties" and "merchant-sovereignties," where "citizen-sovereignties" address the relationship between individuals and governments.[250] In citizen-sovereignties, the individual's "role . . . is that of a stakeholder with a voice" and "a right—if the government is to be called democratic—to participate in its structuring."[251] Merchant-sovereignties, by contrast, describe commercial relations, where individuals' "recourse . . . is simply to take [their] business elsewhere," that is, "to exit."[252]

Exit isn't just easier than voice for individuals with respect to merchant-sovereignties. Exit from allegiance to a *particular* company is also easier than exit from allegiance to a state.[253] In an effort to prevent individuals from being rendered stateless, international law places some limits on states'

ORGANIZATIONS, AND STATES 30 (1970) (defining "voice" as "any attempt at all to change, rather than to escape from, an objectionable state of affairs").

247 *See, e.g.*, *id.* at 15 (explaining that "exit" is fundamentally an economic concept whereby "[t]he customer who, dissatisfied with the product of one firm, shifts to that of another, uses the market to defend his welfare or to improve his position").

248 *See* LESSIG, *supra* note 226, at 288 (arguing that switching sovereigns in "real space" is "costly," but "in cyberspace, moving is not so hard," as evidenced by the ease with which people can switch video games). *But see id.* at 290 ("Paradoxically . . . it may be harder to change communities in cyberspace than it is in real space . . . because you must give up everything in a move from one cyber-community to another, whereas in real space you can bring much of it with you."); Cohen, *supra* note 18, at 144 (arguing that platforms "operate with the goal of making clusters of transactions and relationships stickier—sticky enough to adhere to the platform despite participants' theoretical ability to exit and look elsewhere for other intermediation options").

249 *But see infra* notes 260–61 and accompanying text.

250 LESSIG, *supra* note 226, at 287.

251 *Id.*

252 *Id.*

253 *See* HIRSCHMAN, *supra* note 246, at 33 (noting that "the exit option" is nearly unavailable "in such basic social organizations as . . . the state").

ability to denationalize citizens.[254] Companies are under no such restrictions. Any requirements that a company continue its association with particular users are purely contractual, and individuals can be cut off from any and all corporate "sovereigns" if they violate, for example, the terms of service.[255]

Although cessation of the relationship between "merchant-sovereigns" and their users is comparatively easier—from either side—than in citizen-sovereignties, while the relationship exists, the scope of merchant-sovereignties is thinner but broader than in traditional sovereignties. The technology companies govern a smaller—though usually very important—fraction of their users' lives than territorial sovereigns, but their user bases are far broader, stretching well beyond the domain of a single territorial sovereign. Although the companies are only thinly accountable to their users, to the extent that they are accountable at all, it is to *global*, not just national, constituencies. Consider U.S. government surveillance programs. The U.S. government's position is that users abroad who are not U.S. persons have no legal right to protection from U.S. government surveillance.[256] Non-U.S. persons outside the United States are outside the constituency to whom the U.S. government owes legal duties in this context.[257] The technology companies, by contrast, do not and could not get away with (at least without provoking exercise of exit rights) making a similar distinction. They serve worldwide constituencies, and as explained above, their non-U.S. users outnumber their U.S. users.[258]

---

254 *See* G.A. Res. 217 (III) A, Universal Declaration of Human Rights, at 15 (Dec. 10, 1948) ("No one shall be arbitrarily deprived of his nationality . . . ."); RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 211 cmt. e (AM. LAW INST. 1986) (noting that international law "has accepted some limitations on involuntary termination of nationality . . . to prevent statelessness" and protect against denationalization's use as "an instrument of racial, religious, ethnic, or gender discrimination, or of political repression").

255 *See, e.g.*, Katie Benner, *Twitter Suspends 235,000 More Accounts over Extremism*, N.Y. TIMES (Aug. 18, 2016), https://www.nytimes.com/2016/08/19/technology/twitter-suspends-accounts-extremism.html (reporting that from mid-2015 through mid-August 2016, Twitter suspended 360,000 accounts for terrorist or extremist content); *The Twitter Rules*, TWITTER, https://support.twitter.com/articles/18311 [https://perma.cc/9JE9-STB7] (last visited Feb. 8, 2019) ("You may not make specific threats of violence or wish for the serious physical harm, death, or disease of an individual or group of people. This includes, but is not limited to, threatening or promoting terrorism.").

256 *See, e.g.*, Barack Obama, President, U.S., Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), (transcript available at https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence [https://perma.cc/WH6U-B3GE]) ("[T]he legal safeguards that restrict surveillance against U.S. persons without a warrant do not apply to foreign persons overseas.").

257 The Obama Administration nonetheless imposed policy limits on surveillance of non-U.S. persons abroad. *See* Directive on Signals Intelligence Activities, 2014 DAILY COMP. PRES. DOC. 1 (Jan. 17, 2014) (detailing limitations and recognizing that U.S. "signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information").

258 *See supra* notes 96–104 and accompanying text.

In light of the role that technology companies are currently playing, however, understanding them simply as "merchant-sovereignties" is becoming increasingly unsatisfying. Lessig argued over a decade ago that "cyberspace is not yet dominated (or even broadly populated) by citizen-sovereignties. The sovereignties we see so far are all merchant-sovereignties. And this is even more clearly true with the Internet. . . . Our relationship to them is the same as our relationship to McDonald's."[259] Analogizing Google, Microsoft, Facebook, and the other technology companies—especially considered together—to McDonald's no longer seems accurate. It's a gross understatement of the role the companies play. Users' relationships to these companies are not now, if they ever were, purely transactional.

Moreover, even though users have exit rights as to any particular company, it has become extraordinarily difficult to shed *all* corporate citizenship—that is, to opt out of allegiance to *all* of the major technology companies.[260] One may not need any *particular* social media company, but avoiding them all would require cutting oneself off from a significant sphere of social interaction. Similarly, one may avoid Apple, but foregoing both iOS and Android would likely mean returning to a flip phone.[261] Exit rights involve a choice of companies, but not exit from the technology companies—at least not without significant inconvenience and loss of connectivity.

The evolution of the technology companies into Digital Switzerlands may suggest that they have reached an inflection point between merchant-sovereignties and citizen-sovereignties, or more likely that they are coming to embody a middle category, with characteristics of both. The companies do not offer the voting rights characteristic of democratic states, but they are subject to users' exit rights and have broader constituencies than territorial sovereigns. They promise less to their "citizens" but also in certain circumstances defend them against the territorial governments that both promise and demand more.

If it is correct that the companies are acquiring at least some characteristics of citizen-sovereignties, then it is worth asking how they can be pushed toward the other values expected and demanded of such entities. The next Section turns to those public-law values concerns.

---

259 LESSIG, *supra* note 226, at 287.

260 *See* SCHNEIER, *supra* note 44, at 58 (2015) (analogizing technology companies to "feudal lords" and arguing that "[w]e might prefer one feudal lord to the others[,] . . . distribute our allegiance among several of these companies, or studiously avoid a particular one we don't like," but "it's becoming increasingly difficult to not pledge allegiance to at least one of them").

261 *See* James Vincent, *99.6 Percent of New Smartphones Run Android or iOS*, VERGE (Feb. 16, 2017, 6:11 AM EST), https://www.theverge.com/2017/2/16/14634656/android-ios-market-share-blackberry-2016 [https://perma.cc/HK4J-AUGQ].

C. *Public-Law Values*

To the extent that technology companies are acting in ways that suggest equivalence with states, should they be held responsible for the public-law values demanded of (at least democratic) governments?[262] Public-law values include accountability, transparency, fairness or due process, and protection of privacy and security.[263] Scholars have long advocated extending the public-law values that democratic governments serve to at least *some* private actors.[264] In particular, significant concerns about the extent to which contracting out government functions to private actors undermines public-law values have led some scholars to argue for making private contractors abide by requirements of,

---

262 *Cf.* David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Rep. on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/38/35, at 14-19 (Apr. 6, 2018) (arguing that tech companies should be guided by human rights law in their approach to content moderation); Eyal Benvenisti, *Foreword: Upholding Democracy amid the Challenges of New Technology: What Role for the Law of Global Governance?*, 29 EUR. J. INT'L L. 9, 71-75 (2018) (arguing that tech companies exercise important governance functions and expressing concerns about the efficacy of either self- or governmental regulation to ensure global administrative law values); Jon D. Michaels, *Running Government Like a Business . . . Then and Now*, 128 HARV. L. REV. 1152, 1180-81 (2015) (reviewing NICHOLAS R. PARILLO, AGAINST THE PROFIT MOTIVE: THE SALARY REVOLUTION IN AMERICAN GOVERNMENT, 1780–1940 (2013) (positing that because dominant businesses in some sectors, including technology companies, "essentially control resources, networks, and services that are of vital importance to large segments of the American public," which "interacts with those firms almost out of necessity (rather than choice)[,] . . . there might well be reason to insist that they accept corresponding *public* responsibilities"); K. Sabeel Rahman, *Artificial Sovereigns: A Quasi-Constitutional Moment for Tech?*, LAW & POLITICAL ECON. (June 15, 2018), https://lpeblog.org/2018/06/15/a-quasi-constitutional-moment-for-tech [https://perma.cc/YTR8-XLCU] ("Regulating and responding to new technologies and modern forms of economic and political power . . . represent a variation on familiar questions of public law and constitutional design: how to structure the exercise of potentially arbitrary, state-like power, rendering it contestable, and therefore legitimate.").

263 *See, e.g.*, Laura A. Dickinson, *Regulating the Privatized Security Industry: The Promise of Public/Private Governance*, 63 EMORY L.J. 417, 419 (2013) (identifying "core public values" as including "the procedural values of global administrative law: public participation, transparency, and accountability"); Eichensehr, *supra* note 74, at 516-21 (arguing for including privacy and security among public-law values in the cybersecurity context); Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 HARV. L. REV. 1285, 1285 (2003) (listing the "democratic norms of accountability, due process, equality, and rationality"); Benedict Kingsbury, Nico Krisch & Richard B. Stewart, *The Emergence of Global Administrative Law*, LAW & CONTEMP. PROBS., Summer/Autumn 2005, at 15, 17 (defining global administrative law in terms of mechanisms to ensure "global administrative bodies . . . meet adequate standards of transparency, participation, reasoned decision, and legality," as well as "effective review").

264 For example, global administrative law, which focuses on concerns about institutional compliance with what I here call public-law values, casts a broad net in defining relevant bodies to include not just "formal intergovernmental regulatory bodies," but also "hybrid public-private regulatory bodies, and some private regulatory bodies exercising transnational governance functions of particular public significance." Kingsbury, Krisch & Stewart, *supra* note 263, at 17; *see id.* at 22 (providing the International Standardization Organization as an example of a private regulatory body); *see, e.g.*, Benvenisti, *supra* note 263, at 71-75 (discussing tech companies in the context of global administrative law).

for example, transparency and accountability that would otherwise apply only to governments.[265] Others have extended the argument for applying public law obligations beyond formal contractors to private actors involved in informal partnerships with governments.[266] In a recent article, I argued for extending public values concerns and responsibilities still further to encompass companies in the cybersecurity sphere when they fulfill quintessential public functions, like transnational crime control, foreign policy, and national defense.[267]

All of these prior arguments for the application of public-law values to private parties rest on the nature of the functions that the private parties are performing: public-law values apply where the private actors are performing public functions, defined either by direct outsourcing from governments or by the inherent nature of the functions. It is not clear that the companies' actions as "Digital Switzerlands"—actions like challenging government efforts to access users' information and seeking to disclose information about government information requests—are public functions. Thus, the function-based or conduct-based theories previously used to justify applying public-law values to private parties may not have the same purchase.

If public-law values are to be applied to companies playing the role of Digital Switzerlands, a new theory may be necessary. One possible justification could come in a shift from a function-based understanding of when public-law values should attach to a status-based understanding.[268] This theory would

---

265 *See, e.g.*, Laura A. Dickinson, *Public Law Values in a Privatized World*, 31 YALE J. INT'L L. 383, 403-04 (2006) (proposing extending public-law values to private parties via government contract requirements); Freeman, *supra* note 263, at 1315 (proposing that Congress by legislation could require private parties to comply with public-law values); Martha Minow, *Public and Private Partnerships: Accounting for the New Religion*, 116 HARV. L. REV. 1229, 1266-69 (2003) (detailing four models through which private parties performing public functions can be held accountable); Paul R. Verkuil, *Public Law Limitations on Privatization of Government Functions*, 84 N.C. L. REV. 397, 468 (2006) ("When private contractors perform inherent government functions, they jeopardize core values of public law and weaken government's capacity to do the common good.").

266 *See* Michaels, *supra* note 43, at 947-48, 952-53 (discussing ways in which corporations engaged in informal intelligence partnerships with the government can be harnessed to increase accountability).

267 *See* Eichensehr, *supra* note 74, at 475-78.

268 International law scholars may find it helpful to analogize to the difference between types of official immunity: the functional immunity *ratione materiae* covers a government official's official conduct while in office, while the status-based immunity *ratione personae* covers all actions of a high-ranking government official while that person is in office. *See, e.g.*, LORI FISLER DAMROSCH & SEAN D. MURPHY, INTERNATIONAL LAW CASES AND MATERIALS 880 (6th ed. 2014) (discussing the different types of immunity and noting that after high-ranking officials leave office, their immunity drops from immunity *ratione personae* to immunity *ratione materiae*). The Supreme Court has deployed a similar status-based approach to determining the applicability of constitutional rights. In *Marsh v. Alabama*, the Supreme Court held that the First and Fourteenth Amendments barred enforcement of a ban on distribution of religious leaflets in a privately owned company town. 326 U.S. 501, 507-09 (1946). The ability of the town's residents to engage in free communication, the Court explained, was sufficiently important that constitutional rights attached, despite the fact that town was run by a private, rather than a public, entity. *Id.* at 508-09.

focus not on assessing whether the companies' actions are public functions, but rather on extending basic public-law values requirements to private entities that attain a certain kind of relationship to individuals and governments, namely significant power over individuals and comparable power to governments.[269] Put another way, if and when certain private parties attain government-like status, then they should also acquire government-like responsibilities.

What would it mean in practice for the companies to implement public-law values? Several existing examples provide some models for how the companies could do so, and how practices could be generalized. One example is transparency reports.[270] Google pioneered the transparency report in 2010,[271] followed by Twitter in 2012.[272] The practice has since expanded to technology companies around the world,[273] and the reports routinely include information on, for example, government requests for user account information and National Security Letters, as well as the companies' response to such requests, where permitted.[274] The transparency reports, as the name suggests, serve the public-law value of transparency. Transparency applies to governments

---

269 One way to understand this trigger would be to deploy a "bundle of sticks" conception of sovereignty, somewhat akin to property law's familiar conception of property as a "bundle of sticks." *See, e.g.*, Anthony Sammons, *The "Under-Theorization" of Universal Jurisdiction: Implications for Legitimacy on Trials of War Criminals by National Courts*, 21 BERKELEY J. INT'L L. 111, 114 (2003) ("[T]he analogy of property as a 'bundle of sticks' provides a useful framework for appreciating the present balance between state sovereignty and the international legal order."); Celia R. Taylor, *A Modest Proposal: Statehood and Sovereignty in a Global Age*, 18 U. PA. J. INT'L ECON. L. 745, 754 (1997) (proposing a "functionalist conceptualization of sovereignty" modeled on property law's "'bundle of sticks' that are divisible and transferable"). The question then becomes at what point does a private actor possess a sufficient number of—or sufficiently important—"sovereignty sticks" for obligations based on public-law values to attach to that actor. Thanks to Sean Murphy for suggesting this framing.

270 *See supra* note 220 and accompanying text.

271 *See* David Drummond, *Tools to Visualize Access to Information*, GOOGLE: PUB. POLICY BLOG (Sept. 21, 2010), https://publicpolicy.googleblog.com/2010/09/tools-to-visualize-access-to.html [https://perma.cc/Z4A7-PG5P] (describing the first transparency report, which focused on government requests to remove content and government-caused outages in Google services).

272 *See* Jeremy Kessel, *Twitter Transparency Report*, TWITTER: BLOG (July 2, 2012), https://blog.twitter.com/official/en_us/a/2012/twitter-transparency-report.html [https://perma.cc/K8TA-BSE7] (announcing Twitter's first transparency report, which included information on government requests for user information, government requests to "withhold content," and copyright takedown notices).

273 For a database of companies that release transparency reports, see *Transparency Reporting Index*, ACCESS NOW, https://www.accessnow.org/transparency-reporting-index [https://perma.cc/8KLY-4AVK] (last visited Feb. 8, 2019). *See also* GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/ [https://perma.cc/S3GC-9TBZ] (last visited Feb. 8, 2019) (providing a "non-exhaustive list of transparency reporting efforts").

274 *See, e.g.*, *Report on Government and Private Party Requests for Customer Information: July 1 - December 31, 2016*, APPLE (2016), https://images.apple.com/legal/privacy/transparency/requests-2016-H2-en.pdf [https://perma.cc/ZCF9-CHSH]; *U.S. National Security Orders Report*, MICROSOFT, https://www.microsoft.com/en-us/about/corporate-responsibility/fisa [https://perma.cc/SK54-GSD9] (last visited Feb. 8, 2019) (providing data on Foreign Intelligence Surveillance Act Orders and National Security Letters).

through, for example, freedom of information laws and requirements to publish proposed regulations for comment.[275] These legal requirements do not apply to private actors,[276] but nonetheless, the companies have taken it upon themselves to promote a measure of transparency.[277]

Another example of companies attempting to serve public-law values is the way they approach right-to-be-forgotten requests. The companies have internal procedures to guide their determinations about whether to delist content pursuant to a request from an individual.[278] Google's *EU Privacy Removal* form explains that the company "will balance the privacy rights of the individual concerned with the interest of the general public in having access to the information, as well as the right of others to distribute the information," and the company "may decline to remove certain information" in which there is a public interest, including "information about financial scams, professional malpractice, criminal convictions, or public conduct of government officials."[279] Microsoft's Bing delisting form similarly explains that "Bing must balance individual privacy interests against the public interest in protecting free expression and the free availability of information, consistent with European law."[280] These regularized processes attempt to provide a measure of due process to both takedown requesters and other users who may have an interest in accessing the information. Similarly, the companies also provide means for users to appeal takedowns of the content they post.[281] Although these measures have been criticized,[282] the fact that the companies are attempting to standardize processes, as opposed to treating

275 *See* Administrative Procedure Act of 1946 § 4, 5 U.S.C. § 553 (2012) (setting out procedures for notice and comment rulemaking); Freedom of Information Act of 1967, 5 U.S.C. § 552 (2012) (setting out public information requirements and procedures).

276 *See, e.g.*, Nina A. Mendelson, *Six Simple Steps to Increase Contractor Accountability*, *in* GOVERNMENT BY CONTRACT: OUTSOURCING AND AMERICAN DEMOCRACY 241, 249-50 (Jody Freeman & Martha Minow eds., 2009) (explaining that the Administrative Procedure Act and Freedom of Information Act do not reach government contractors).

277 *But see* Cohen, *supra* note 18, at 175 ("[A]lthough the major platforms widely publicize information about the takedown notices they receive from copyright owners and, to the extent permitted, about government production requests, they provide no comparable public transparency about the details of their own automatic filtering and manipulation.").

278 For a detailed overview of how the companies approach content moderation generally, see Klonick, *supra* note 136, at 1631-48.

279 *EU Privacy Removal*, *supra* note 216.

280 *Request to Block Bing Search Results in Europe*, *supra* note 216.

281 *See* Klonick, *supra* note 136, at 1647-48 (detailing the companies' appeal processes); *How to Appeal*, ONLINECENSORSHIP, https://onlinecensorship.org/resources/how-to-appeal [https://perma.cc/PQS5-JYBH] (last visited Feb. 8, 2019) (collecting information on how to appeal content takedowns and blockages by sites including Facebook and Twitter).

282 *See, e.g.*, Kaye, *supra* note 262, at 10-14 (expressing concerns about, inter alia, vague rules on content moderation, inadequate notification and appeal processes, and limited transparency about content removals).

requests in an ad hoc fashion, suggests a move toward a measure of due process—albeit one not legally required for nongovernmental actors.[283]

Numerous mechanisms could drive the companies to apply public-law values to their actions. Market-based competition may be one factor. If competitor companies undertake a certain practice, like publication of transparency reports, and companies believe users value the practice, then competitive pressure will drive additional companies to undertake the practice. Another mechanism is diffusion of corporate social responsibility norms. To the extent that these norms incorporate public-law values, then they can also push companies toward adoption of practices that serve values like transparency and due process.[284] For example, Microsoft's transparency reports are already located under the corporate social responsibility heading on the company's website,[285] along with issues like environmental sustainability and human rights.[286]

Another mechanism that might drive the companies to implement public-law values is the perception that certain practices, like requiring governments to produce legal process before the company turns over account information, have become the industry standard. The companies' interest in complying with industry-standard practices may be partly competitive, as discussed above, but it may also be a calculation about legal risk. Tort liability often depends on whether a company has engaged in a commercially reasonable practice, and to the extent that a company is out of step with practices that have become industry standard, it may open itself to claims by individuals who suffer harm from the company's failure to align itself with the mainstream practices. This mechanism still involves voluntary compliance by the companies with public-law values, but it is voluntary compliance with the threat of conversion of a practice into a legal requirement in a future lawsuit.

---

283 For additional suggestions about how the companies could apply due process to users, see MICHAELS, *supra* note 81, at 7.

284 For example, the Global Network Initiative (GNI) launched in 2008 to bring together companies, academics, civil society organizations, and investors to address issues regarding how companies handle government demands that impact users' privacy and freedom of expression. *See* MACKINNON, *supra* note 18, at 179-81 (describing GNI's founding); *see also* GLOB. NETWORK INITIATIVE, GNI PRINCIPLES ON FREEDOM OF EXPRESSION AND PRIVACY (2017), https://globalnetworkinitiative.org/gin_tnetnoc/uploads/2018/04/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf [https://perma.cc/6NJ6-K2JK]; *Portfolio*, GLOB. NETWORK INITIATIVE, http://globalnetworkinitiative.org/participants/index.php [https://perma.cc/S5QT-S7TR] (last visited Feb. 8, 2019) (listing corporate, academic, civil society, and investor participants). For critiques of GNI, see, for example, Anupam Chander, *Googling Freedom*, 99 CALIF. L. REV. 1, 38 (2011), which notes four critiques, including the likelihood that many companies will not join and that the voluntary commitments will fail in the face of government imposed legal requirements.

285 *U.S. National Security Orders Report*, *supra* note 274.

286 *Environmental Sustainability*, MICROSOFT, https://www.microsoft.com/en-us/corporate-responsibility/environmental-sustainability [https://perma.cc/Z2WW-CN58] (last visited Feb. 8, 2019); *Human Rights*, MICROSOFT, https://www.microsoft.com/en-us/corporate-responsibility/human-rights [https://perma.cc/27CL-CZ6R] (last visited Feb. 8, 2019).

In recent articles, scholars have proposed different means of imposing broad-based legal regulation on the companies in ways that would serve at least some public-law values. For example, Jack Balkin and Jonathan Zittrain have proposed making online service providers "information fiduciaries."[287] While traditional fiduciaries owe duties of care and loyalty to their clients,[288] Balkin posits that the exact nature of the duties imposed on online service providers should vary based on the nature of their business.[289] The information fiduciary status could arise through direct imposition of legal regulations establishing the fiduciary duties or legal incentives, like "tax breaks, safe harbors, [or] legal immunities" to entice companies to self-designate as information fiduciaries.[290] K. Sabeel Rahman, on the other hand, has proposed regulating "online-enabled infrastructure," including Google, Facebook, and Amazon, as public utilities.[291] He envisions a range of possible regulations, for example, to prohibit discrimination or require the companies to act consistent with common carrier duties.[292]

While there is much to recommend these proposals as controls on the relationship between companies and *users*, it is far less clear that they could

---

287 *See* Balkin, *supra* note 206, at 1209 (defining an "information fiduciary" as "a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of their relationship"); Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346 [https://perma.cc/W6MB-ZXNG] (discussing why and how to make online platforms information fiduciaries); *see also* Balkin, *supra* note 206, at 1223-24 (setting out three criteria for determining when a business is an information fiduciary).

288 Balkin, *supra* note 206, at 1207-08.

289 *Id.* at 1229.

290 *Id.*; *see also* Jonathan Zittrain, *How to Exercise the Power You Didn't Ask For*, HARV. BUS. REV. (Sept. 19, 2018), https://hbr.org/2018/09/how-to-exercise-the-power-you-didnt-ask-for [https://perma.cc/W233-C7Q6] (arguing that "[i]deally, companies would become fiduciaries by choice, instead of by legal mandate" in response to, for example, "U.S. federal law offering relief from the existing requirements of individual states if companies opt in to fiduciary status"); Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering [https://perma.cc/XRQ4-AR2C] (proposing that to incentivize online platforms to become information fiduciaries, "the government could offer tax breaks or certain legal immunities for those [companies] willing to step up toward an enhanced duty to their users").

291 Rahman, *supra* note 2, at 1669, 1672; *see also* GANESH SITARAMAN, GREAT DEMOCRACY INITIATIVE, REGULATING TECH PLATFORMS: A BLUEPRINT FOR REFORM 5-6 (2018), https://greatdemocracyinitiative.org/wp-content/uploads/2018/03/Regulating-Tech-Platforms-final.pdf [https://perma.cc/SM2J-V9H4] (discussing how to adapt traditional public utilities regulations to Internet platforms). *But see* BALKIN, *supra* note 83, at 7 (criticizing proposals for regulating social media companies as public utilities); Peter Swire, *Should the Leading Online Tech Companies Be Regulated as Public Utilities?*, LAWFARE (Aug. 2, 2017, 9:00 AM), https://www.lawfareblog.com/should-leading-online-tech-companies-be-regulated-public-utilities [https://perma.cc/7T3U-LSVP] (discussing arguments in favor of regulating tech companies as public utilities but also highlighting reasons the public utility model is problematic).

292 Rahman, *supra* note 2, at 1674, 1677.

effectively address the relationship between companies and *governments* that the Digital Switzerlands concept primarily addresses.[293] For the many problems stemming from how companies benefit from and exploit user data, the prospect of regulation is in some ways a classic type of fix: government officials looking down upon the problematic actions of the companies can step in to impose limits on what companies can do to users. But what happens when the government itself is a threat to users? In that circumstance, government regulation is a far less attractive solution.

It is both less plausible as a descriptive matter and less desirable as a normative matter to craft regulations that empower companies to check the government. Crafting regulations that would require the companies to act for the benefit of users, even against the government, could well be antithetical to the interests of (at least some powerful parts of) the government.[294] Consider Microsoft or Google bolstered by a fiduciary duty of care and loyalty toward their users that they understand to *legally obligate* them to challenge government requests for information, resist government pushes to bypass product security features, and disclose the maximum possible amount of information about government information requests. A legal obligation to defend public-law values would make the companies more of a thorn in the side of governments. Government actors—at least executive branch officials—then have diminished incentives to support proposals to obligate companies to act as Digital Switzerlands.

But government regulation could take another, more objectionable form. Allowing the government to define how companies should protect user interests *in the government-versus-user* context could well become the vehicle not for empowering the companies to defend users, but for undermining their ability to do so effectively. Think of a regulation requiring backdoors to compromise encryption. In other words, putting the government in a position to regulate the company–government relationship is likely to result (unsurprisingly) in regulations that favor the government's interests, rather than regulations that strengthen companies' ability to robustly check the government.

Any legislative effort to impose generalized regulatory schemes to mandate consumer protection against governments would likely face opposition from the *companies* as well. The regulations would no doubt be somewhat burdensome, and being legally required to take actions to defend

---

293 As currently formulated, I do not understand the extant regulatory proposals to reach the issues that this Article primarily addresses, and, as this Section explains, for good reason.

294 *Cf.* Ryan Calo, *Can Americans Resist Surveillance?*, 83 U. CHI. L. REV. 23, 40-41 (2016) (arguing that corporate promises to resist government demands for information are unlikely to be effective because "the same government that is asking for the data" is responsible for enforcing and is thus unlikely to enforce the promise).

users against the government would take away the marketing value of the companies' current willingness to undertake such actions.

Regulation to protect against government action is even less likely now in the United States where any proposals that require legislative action fall subject to the paralysis and gridlock that characterize the political branches of the federal government. With a President determined to dismantle the regulatory state,[295] putting faith in the prospect of new regulation as a generalized solution is a dicey proposition—and all the more so when regulation would empower companies to resist the government.

On the other hand, specialized regulatory requirements may be more likely, especially when addressed to the behavior of *foreign* governments. Limiting *other* governments does not produce the same disincentives involved in expecting the U.S. Congress and President to check the U.S. government. One example is a pending congressional bill, the Honest Ads Act, which would require Internet companies to disclose the purchasers of online political ads.[296] The bill is a direct reaction to the disclosures about Russian purchases of advertising on Internet platforms to influence the 2016 election.[297] Imposition of targeted regulation, or even threats of such regulation, can play a useful role in mitigating the risks of passivity that can attend a posture of neutrality,[298] and it would serve the public values of transparency and accountability.[299] To date, several tech companies have announced their support for the bill,[300] and

---

295 *See, e.g.*, JON D. MICHAELS, CONSTITUTIONAL COUP: PRIVATIZATION'S THREAT TO THE AMERICAN REPUBLIC 13 (2017) ("[President Trump] pays no fealty to the State. Quite the opposite: he promised to 'drain the swamp,' meaning the Washington bureaucracy . . . .").

296 Honest Ads Act, S. 1989, 115th Cong. (2017); *see also* Kenneth P. Vogel & Cecilia Kang, *Senators Demand Online Ad Disclosures as Tech Lobby Mobilizes*, N.Y. TIMES (Oct. 19, 2017), https://www.nytimes.com/2017/10/19/us/politics/facebook-google-russia-meddling-disclosure.html (describing the Honest Ads Act).

297 *See* Vogel & Kang, *supra* note 296 ("[I]n the run-up to the 2016 election, Facebook sold more than $100,000 worth of ads to a Russian company linked to the Kremlin, while Google sold at least $4,700 worth of ads to accounts believed to be connected to the Russian government."); *see also Election Hearings*, *supra* note 222, at 30-31 (statement of Sean J. Edgett, Acting Gen. Counsel, Twitter, Inc.) (discussing ad purchases on Twitter); *id.* at 12-14 (statement of Colin Stretch, Gen. Counsel, Facebook) (describing Internet Research Agency ad purchases and impact on Facebook); *id.* at 43 (statement of Kent Walker, Senior Vice President & Gen. Counsel, Google) (describing ad purchases on Google-owned sites); Elliot Schrage, *Hard Questions: Russian Ads Delivered to Congress*, FACEBOOK: NEWSROOM (Oct. 2, 2017), https://newsroom.fb.com/news/2017/10/hard-questions-russian-ads-delivered-to-congress [https://perma.cc/6QMT-Y8SM] (reporting ad spending and impressions).

298 *See supra* notes 195–98 (discussing how neutrality can foster passivity).

299 Imposition of such targeted regulations somewhat ironically bolsters neutrality, while at the same time highlighting the continued subordination of the companies to national government regulators, and thus challenging the other prong of the Digital Switzerlands analogy—the claim to parity with states.

300 *See* Tom Burt, *Announcing the Defending Democracy Program*, MICROSOFT: MICROSOFT ON THE ISSUES (Apr. 13, 2018), https://blogs.microsoft.com/on-the-issues/2018/04/13/announcing-the-defending-democracy-program [https://perma.cc/5EEH-9EVC] (announcing Microsoft's support for the Honest Ads Act); Mark Zuckerberg, FACEBOOK (Apr. 6, 2018), https://www.facebook.com/

for good reason: support is consistent with the model described above whereby the companies will generally not oppose a government's actions where the government is clearly allied with users.[301]

In the medium term, then, the most promising avenues for getting the companies to abide by public-law values are those that are already bearing some fruit. Competitive pressures, corporate social responsibility norms, evolving industry standards, and threats of targeted regulation are imperfect mechanisms, but they are feasible avenues of progress.

D. *Stability and Sustainability*

Finally, companies' willingness to play the role of "Digital Switzerlands" may be highly contingent. There is currently business value in championing privacy, defending users against governments, and announcing neutrality between territorial governments.[302] But circumstances may shift, as they have in the past, and companies may come to see greater advantages in alliances with governments, instead of neutrality, and in cooperation, rather than resistance.[303] Thus, the question becomes if there is value in having technology companies be or at least aspire to be Digital Switzerlands, how can their role be stabilized to prevent backsliding?

The companies' willingness to play the Digital Switzerlands role seems to depend, as argued in Section II.C, on the relative positions of users and governments. The companies appear willing to resist governments when they have viable legal arguments and can plausibly claim to be on the side of users against governments. One major threat to the stability of the Digital Switzerlands model would be a shift among users toward alignment with governments. Such a shift might be driven by an exogenous shock, like a significant terrorist attack or frequent lower-level terrorist attacks. Users might react to exogenous shocks by exhibiting greater tolerance for government requests, for example, to access encrypted communications or to surveil the content of user accounts. Though often described as a tradeoff between privacy and security, it is more accurate to say that users might alter their security–security tradeoff—shifting from concern about security *from* governments to greater concern about the security *of* governments in the sense that those governments provide physical protection to their people. User concern about government surveillance could also dissipate not with a bang, but with a whimper,

---

zuck/posts/10104784125525891 [https://perma.cc/KM4E-AG9J] (announcing that Facebook supports passage of the Honest Ads Act).

301 *See supra* notes 209–10 and accompanying text.

302 *Cf.* SCHNEIER, *supra* note 44, at 207; Calo, *supra* note 294, at 39 ("[T]he Snowden revelations and subsequent global reaction to the NSA's spying capabilities have invigorated privacy as a competitive differentiator.").

303 *See, e.g.*, *infra* notes 316–17 and accompanying text.

embracing fatalism about ubiquitous surveillance and monitoring. In that circumstance, companies may see little value in resisting governments.[304]

Another type of exogenous shock could be significantly increased pressure on the companies by governments around the world.[305] Such pressure might be spurred, for example, by perceived threats to the ruling regime or periods of particular sensitivity to users' critiques of the government.[306] Increased government pressure could manifest in different ways, including, for example, threats to ban companies' products, embroil the companies in costly legal proceedings, use competition law to break up the companies, or take action against the companies' assets or personnel in a country unless the companies cease challenging the government. These scenarios are not farfetched. Authorities in countries like Brazil and Italy have arrested company executives for failing to comply with government requests or orders.[307] This type of exogenous shock does not depend on a shift in the position of users, but rather because it would increase the costs to companies of continuing to resist governments, it could cause companies to behave differently—that is, to cease resistance and cooperate with governments. Such a choice would be a violation of the Digital Switzerlands model, but if time limited and geographically limited, some number of deviations would not cause the model's collapse.

Assuming the model is vulnerable to various exogenous shocks, what can be done to reinforce and entrench it?

---

304 Such a movement may be underway with respect to government-directed content controls. *See, e.g.*, Manjoo, *supra* note 214 (noting, in discussing Google's reported plan to relaunch a censored search engine in China, that many governments now engage in content controls and that companies like Amazon, Apple, and Microsoft already do business in China).

305 Increased government pressure could be the result of either endogenous or exogenous reasons. On the endogenous side, governments might increase pressure on companies in response to a shift in position of users away from companies and toward the governments. That shift is endogenous to the model described in Section II.C. This paragraph focuses instead on *exogenous* reasons that government pressure might increase.

306 *See, e.g.*, Jonathan Kaiman, *China Cracks Down on Dissent Ahead of Tiananmen Anniversary*, GUARDIAN (May 13, 2014, 11:50 EDT), https://www.theguardian.com/world/2014/may/13/china-cracks-down-dissent-tiananmen-anniversary [https://perma.cc/5EV4-E33Q] (detailing Chinese government crackdowns surrounding the twenty-fifth anniversary of Tiananmen Square).

307 *See, e.g.*, RONALD J. DEIBERT, BLACK CODE: SURVEILLANCE, PRIVACY, AND THE DARK SIDE OF THE INTERNET 109 (2013) (discussing arrests of a Google official in Brazil and charges against Google executives in Italy relating to Google's failure to remove videos from its services); *see also* Jonathan Watts, *Brazilian Police Arrest Facebook's Latin America Vice-President*, GUARDIAN (Mar. 1, 2016, 10:35 EST), https://www.theguardian.com/technology/2016/mar/01/brazil-police-arrest-facebook-latin-america-vice-president-diego-dzodan [https://perma.cc/478U-5RML] (reporting that a Facebook executive was arrested in Brazil for questioning regarding Facebook subsidiary WhatsApp's alleged noncompliance with a court order requiring disclosure of user communications, which the company avers that it does not store); Jacob Kastrenakes, *Brazil Orders Release of Facebook Executive Arrested in WhatsApp Dispute*, VERGE (Mar. 2, 2016, 9:40 AM EST), https://www.theverge.com/2016/3/2/11145494/facebook-vp-being-released-brazil-whatsapp-dispute [https://perma.cc/TF2A-MLCN] (reporting that the Facebook executive was released a day after his arrest).

One means to drive entrenchment is transparency. The transparency reports that companies issue about government requests for content enable at least some oversight and monitoring of government actions and of the companies' reactions. Although publication of the reports is entirely voluntary, various pressures have pushed companies toward publication and similarly militate against cessation of the practice. Some of the pressure comes from competitors: publishing transparency reports has become an industry standard.[308] Amazon, which was comparatively slow to begin publishing transparency reports,[309] received criticism for failing to do so.[310]

Civil society groups also exert pressure on the companies. For example, since 2011,[311] the Electronic Frontier Foundation has published an annual report entitled *Who Has Your Back?* that tracks and compares the performance of technology companies across a variety of metrics, including disclosing government data requests to users, resisting government gag orders prohibiting disclosure, and following industry-wide best practices, including publication of transparency reports.[312] In a recent report, Amazon and WhatsApp received particular criticism among technology companies, and earned only two out of five possible "stars," due to failures to, for example, commit to notifying users of government data requests.[313]

Consumers and investors can also pressure companies to maintain strong security practices and challenge government demands with respect to users. Civil society groups' monitoring of companies' practices—a naming and shaming mechanism—fosters the ability of informed consumers and investors

---

308 *See, e.g.*, Lucy Schouten, *How Google Became a Champion for Government Transparency*, CHRISTIAN SCI. MONITOR (July 19, 2016), https://www.csmonitor.com/Technology/2016/0719/How-Google-became-a-champion-for-government-transparency (publishing transparency reports has "become an all-but-expected practice among major technologies with a Fortune 500 ranking").

309 Amazon issued its first transparency report in June 2015. Ben Fox Rubin, *Amazon Discloses Transparency Report for First Time*, CNET (June 12, 2015, 7:07 PM PDT), https://www.cnet.com/news/amazon-discloses-transparency-report-for-first-time.

310 *See, e.g.*, Taylor Soper, *ACLU Technologist: 'Amazon Has Escaped the Transparency Spotlight'*, GEEKWIRE (Mar. 12, 2015, 6:30 AM), https://www.geekwire.com/2015/prominent-aclu-technologist-chris-soghoian-amazon-has-escaped-the-transparency-spotlight [https://perma.cc/GKK8-LW3K] (reporting ACLU Principal Technologist Chris Soghoian's public criticism of Amazon for failing to publish transparency reports); Zack Whittaker, *Amazon Doesn't Want You to Know How Many Data Demands It Gets*, ZDNET (Mar. 19, 2015, 10:34 PDT), http://www.zdnet.com/article/amazon-dot-com-the-tech-master-of-secrecy [https://perma.cc/LHR3-87GT] (criticizing Amazon's failure to publish transparency reports).

311 For the first report, published in 2011, see *When the Government Comes Knocking, Who Has Your Back?*, ELEC. FRONTIER FOUND., https://www.eff.org/who-has-your-back-2011 [https://perma.cc/MFG2-VSY9] (last visited Feb. 8, 2019).

312 *See* NATE CARDOZO ET AL., ELEC. FRONTIER FOUND., WHO HAS YOUR BACK? 2017, at 9-11 (2017), https://www.eff.org/files/2017/07/08/whohasyourback_2017.pdf [https://perma.cc/M2JK-JJUC] (detailing rating criteria).

313 *See id.* at 6, 8.

to vote with their feet, choosing service and product providers and potential investment options at least partly based on their security practices. Consumers and investors in the aggregate have the potential to reward and punish companies in the market based on the public stances they take.

Another source of entrenchment of the Digital Switzerlands role could potentially come from governments themselves. This may seem paradoxical. After all, government behavior is monitored incidentally through the companies' transparency policies and checked by the companies' challenges. Nonetheless, it is possible to envision a very privacy protective (probably European) government that might be concerned about protecting its citizens against foreign governments. Such a government could, for example, mandate publication of transparency reports, transforming what is currently a voluntary practice into a legal requirement. Such a regulation, of course, might raise questions about the extent to which one country could mandate disclosure of government requests or orders worldwide, as opposed to just those requested by its own government or by all governments with respect to its own citizens. A legal mandate for publication of transparency reports could bolster companies' legal position vis-à-vis governments in other countries that might seek to restrict publication of government request information.

All of these mechanisms may help to entrench the Digital Switzerlands model, but they are fragile and incomplete. The model remains vulnerable to shocks that could reshape the relationship between users, governments, and technology companies.

CONCLUSION

Considering the potential role of U.S. technology companies as Digital Switzerlands reveals several insights, some specific to the current situation and others more generalizable.

The Digital Switzerlands concept is aspirational and may remain that way. With the exception of Denmark's dispatch of a digital ambassador to the companies,[314] states do not regard the companies as peers, and the companies lack the territory and monopolization of the use of violence within territory that are required for statehood. But they have attained some measures of power comparable to states, and they continue—in circumstances of their choosing—to resist governments, and to do so successfully in many cases.

For technology users, the companies are powerful regulators, but also powerful defenses against government regulators. Dual sovereignties may ultimately help to protect users from governments. But in accepting dual sovereigns, it is important to critically evaluate the corporate supplemental sovereigns, which lack

314 *See supra* note 161 and accompanying text.

most of the traditional aspects of democracy that legitimize governments. The companies gain some legitimacy in other ways, including responsiveness to a community of worldwide "constituents," the constant threat by users to exit, defecting to other corporate "sovereigns," and voluntarily undertaking to abide by some public-law values. These features help lend some legitimacy to the companies for the limited purpose of serving as counterweights to traditional governmental sovereigns, but they remain fundamentally undemocratic.

Moreover, embracing the Digital Switzerlands concept may strengthen the companies' will and capacity to resist government regulation of the companies' power over their users—a power that has many troubling aspects.[315] The companies' rising power to counter governments, in other words, may affect their power over users. As the companies' overall power increases, the power of governments over them may decrease, including when it comes to regulating the companies' treatment of users and user data. While it is still too soon to know definitively how the Digital Switzerlands concept will influence the companies' relationship to governments and users, companies' parity with governments on one plane of interaction may ultimately affect others.

At the same time, the companies' embrace of actions consistent with the Digital Switzerlands idea is fragile. The Digital Switzerlands concept is the latest evolution in the companies' role with respect to governments—a role that has changed considerably even in the last decade. The evolution suggests that the likelihood of change is perhaps the most stable feature. And the issue that may cause the companies to abandon pursuit of neutrality may already be on the horizon: companies are taking divergent positions on sales of artificial intelligence and other advanced technologies to nation-state militaries.[316] Such sales would not themselves necessarily violate neutrality, which merely suggests treating states equally. But treating states equally by selling to no militaries may be untenable as a business proposition, whereas treating states equally by selling to all militaries raises serious questions of security and human rights. The need or desire to differentiate between military customers may cause the companies to align themselves with their national government and allied governments in ways that they have avoided so far.[317]

Still, the U.S. technology companies' current pursuit of a posture of neutrality as between governments is a new development in the history of powerful companies. Although it is an imperfect neutrality given the companies' ongoing association with the United States, the Digital

---

315 *See supra* note 6 (discussing concerns with the company–user relationship and collecting sources).

316 *See supra* note 142 and accompanying text (discussing the companies' diverging positions on sales to the U.S. military).

317 *See supra* notes 75–76 and accompanying text (discussing how the tech companies so far differ from traditional military contractors).

Switzerlands concept nonetheless suggests a different kind of role private actors can play: denationalized, global, powerful due to mass appeal to individuals, and willing to stand up to traditional territorial sovereigns in the name of the users that are necessary to maintain the companies' power. Even if the Digital Switzerlands model ultimately breaks down for the U.S. technology companies, a similar model might arise with other companies or other sectors in the future. Industries that have global user bases, tight ties to (nongovernmental) customers, and significant resources could ultimately stand as new "Switzerlands," whether digital or not.