RAISING THE STAKES: CREATING AN INTERNATIONAL SANCTION TO GENERATE CORPORATE COMPLIANCE WITH DATA PRIVACY LAWS

Jonathan Trebble-Greening*

In the current framework of human rights, data privacy is finding its home as an independent human right, separate from its historical home under the umbrella of general privacy. However, there is no consistent system or standard for defining this right, and different regions require substantially different levels of protection. This inconsistency has allowed for corporations, by way of their executive officers, to avoid or completely ignore the requirements imposed by many countries. Moreover, the penalties in many regions are not severe enough to incentivize corporations to change their behavior. The lack of a truly global system and standard for enforcing this right, and the specific lack of pressure on the officers that direct corporate policy, has allowed data privacy violations to go severely under-checked.

This Note seeks to provide a novel solution for tackling corporate holdup in complying with data privacy laws. This Note examines the historical roots of data privacy as a human right, discusses its similarity to resources that have been considered public utilities, and provides examples of instances where the right to data privacy has been ignored by corporate officers. By modifying the United Nations' existing sanction procedure and jurisdiction, this Note proposes that the United

* J.D. Candidate 2020, Columbia Law School; B.S. 2013, University of Georgia. Many thanks to Professor Sarah Cleveland for serving as my advisor during the writing of this Note. Thanks also to Professor Amal Clooney for her early guidance in selecting a Note topic and for her continued support. Sincerest gratitude to the staff of the *Columbia Business Law Review* for their thoughtful comments and edits in preparing this Note for publication. Finally, utmost thanks to my parents, Bill and Jo, and my brother, Reed, for their unwavering love and support – now and always.

Nations would be able to target corporate officers individually for their roles in data privacy violations. By leveraging personal liability for noncompliance, the United Nations could generate a global sense of accountability to the modern, human right to privacy in one's personal data.

"Privacy and security are the ultimate shared responsibility and everyone, including governments, companies, and citizens, [has] an important role to play."[1]

[1] Charles Arthur, *Google's Jared Cohen Discusses the Digital Future – Live Q&A*, GUARDIAN (Apr. 25, 2013), https://www.theguardian.com/technology/2013/apr/24/google-jared-cohen-digital-future [https://perma.cc/RSH3-MLY5] (quoting Jared Cohen of Google's response to a question).

I. INTRODUCTION

Managing data privacy has never been more important to corporate responsibilities than now. In the wake of data crises like the hack of more than 100 million Target shoppers' credit card and contact information, the hack that exposed all three billion Yahoo users' personal information, and the Equifax hack that revealed more than 147 million users' personal information—including social security numbers—corporate officers have been forced to rethink their companies' strategies for protecting user data.[2] These breaches not only effect financial valuation during a sale or merger; they can also result in substantial lawsuit settlements and financial penalties.[3]

Yet even in the face of these precedents, many giant data-driven companies continue to fail at protecting users' data.[4] Even as regulations and laws that cover data privacy more broadly than ever before are emerging globally with increasing frequency[5]—providing companies with improved guidance on how they should be managing user data—commentators have suggested that some companies have circumvented these regulations or even blatantly violated them.[6] This raises the questions of whether the existing

[2] *See* Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO (Dec. 20, 2018), https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html [https://perma.cc/2UQM-2VZ7].

[3] *See id*.

[4] *See, e.g.*, Russell Brandom, *The Facebook Hack Could Be Europe's First Big Online Privacy Battle*, VERGE (Oct. 1, 2018), https://www.theverge.com/2018/10/1/17922946/facebook-breach-gdpr-lawsuit-privacy-commissioner-europe [https://perma.cc/4VRT-RJ8B]; Jon Porter, *Google Accused of GDPR Privacy Violations by Seven Countries*, VERGE (Nov. 27, 2018), https://www.theverge.com/2018/11/27/18114111/google-location-tracking-gdpr-challenge-european-deceptive [https://perma.cc/U5BV-9JKJ].

[5] *See* Ronan Shields, *American Data Privacy Laws Are a Matter of How, Not If*, ADWEEK (Oct. 7, 2018), https://www.adweek.com/programmatic/privacy-laws-are-a-matter-of-how-not-if/ [https://perma.cc/G9L9-U4W5/].

[6] *See* Brandom, *supra* note 4; *see also* Matt Novak, *Facebook and Google Accused of Violating GDPR on First Day of the New European Privacy Law*,

penalties surrounding data privacy are severe enough and whether a substantive change in policy is warranted. While some of the more recent regulations like the General Data Protection Regulation ("GDPR") in Europe protect member states' citizens by imposing severe financial penalties on corporate rule violators,[7] there is no global deterrent that incentivizes corporate officers to change their companies' policies to better protect user data from misappropriation. Without such a global system, it is likely that corporate data privacy practices will not prioritize user information protection or prevent human rights violations.

Part II of this Note addresses the current state of data privacy rights with a particular focus on the obligations imposed on companies in the European Union ("EU"), the United States, and the United Nations ("UN"). This Part also explains how data privacy came to be widely acknowledged as a human right. Part III addresses a variety of issues relating to the sanctioning of corporate officers, including the historical nature of sanctions and the role that data-driven companies have in the utility regulation scheme. Finally, Part IV of this Note proposes a novel solution for generating top-down compliance with data privacy laws on a global level using the United Nations and sanctions regimes.

II. BACKGROUND ON DATA PRIVACY RIGHTS

Over the past forty years, data privacy has moved to the forefront of the international rights debate. Namely, two key questions have dominated the conversation: (1) what rights do people possess in regards to their own information, and (2) how far does the right to privacy extend?[8] As technology and

GIZMODO (May 25, 2018), https://gizmodo.com/facebook-and-google-accused-of-violating-gdpr-on-first-1826321323 [https://perma.cc/Y5C8-JBSL].

[7] *See GDPR Overview*, GDPREU.ORG, https://www.gdpreu.org [https://perma.cc/E3ZN-EG9H]; *see also* CONSUMERS INT'L, THE STATE OF DATA PROTECTION RULES AROUND THE WORLD: A BRIEFING FOR CONSUMER ORGANISATIONS 5 (2018), https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf [https://perma.cc/RAA5-E62S].

[8] *See* Eve Maler, *Data Privacy Day: Assessing the State of the Privacy Nation in 2019*, GDPR:REPORT (Jan. 29, 2019), https://gdpr.report/news/

the nature of how personal data can be used have evolved in tandem, these rights have been called into question, causing many countries to prioritize their protection.[9]

Especially noteworthy is the gradual transition of data privacy away from being considered a purely privacy-related right toward its inclusion under the broader human rights umbrella.[10] The right to privacy has existed in international doctrine for decades, most notably appearing in Article 12 of the Universal Declaration of Human Rights ("UDHR").[11] However, in the past decade, the increase in data leaks and unauthorized disclosures of personal information has raised questions about data's place in the privacy arena.[12] Moreover, the lack of proactivity by corporations in preventing data privacy violations has raised grave concerns about private data management, which precipitated a dialogue around increasing the government's role in overseeing private data management.[13]

2019/01/29/data-privacy-day-assessing-the-state-of-the-privacy-nation-in-2019/ [https://perma.cc/Q6QZ-LMXW].

[9] *See generally* Oliver Diggelmann & Maria Nicole Cleis, *How the Right to Privacy Became a Human Right*, 14 HUM. RTS. L. REV. 441 (2014); *see also* James Reynolds, *What's Data Protection Got to Do with Human Rights?*, RIGHTSINFO (Aug. 17, 2017), https://rightsinfo.org/whats-data-protection-got-human-rights/ [https://perma.cc/MJF9-3FBJ].

[10] *See* Nithin Coca, *How the Push to Make Data Privacy a Human Right Will Impact Businesses*, TRIPLE PUNDIT (Oct. 22, 2018), https://www.triplepundit.com/special/data-privacy-symantec-series-2018/how-the-push-to-make-data-privacy-a-human-right-will-impact-businesses/ [https://perma.cc/3D5N-C2VZ].

[11] G.A. Res. 217 (III) A, Universal Declaration of Human Rights, at art. 12 (Dec. 10, 1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.").

[12] *See* Valentina Maria Ariemme, *Recent Developments in the Recognition of Digital Privacy as a Human Right*, EUR. TAX STUD., no. 2, 2014, at 78.

[13] Coca, *supra* note 10 ("Companies, particularly in the technology space, have been more reactive than proactive on data privacy. For consumer privacy to really come to the forefront, it is likely that government will also have to play a role—especially in instances where consumers don't have a choice to switch to a privacy-protecting alternative.").

An annual report from the Office of the United Nations High Commissioner for Human Rights linked these data privacy issues to human rights, stating that although data and the internet provide for an improvement of human rights, "[i]n the digital era, communications technologies also have enhanced the capacity of Governments, enterprises and individuals to conduct surveillance, interception and data collection."[14] At the crux of this statement is the idea that when dealing with data transfers and the internet in general, "the rights held by citizens offline must also be protected online."[15] Interestingly, chief executive officers ("CEOs") of some of the companies facing the greatest risk of incurring penalties for data privacy violations are calling for data privacy rights to be recognized as human rights.[16] This response is not altogether surprising, however, considering the breadth of the data these companies know they are collecting—anything from users' musical preferences to their social media contacts may be stored on corporate servers.[17] As

[14] U.N. High Comm'r for Human Rights, The Right to Privacy in the Digital Age, ¶ 2, U.N. Doc. A/HRC/27/37 (June 30, 2014).

[15] Ariemme, *supra* note 12, at 79.

[16] *See Privacy Is "A Human Right": Apple CEO Tim Cook*, MSNBC (Mar. 28, 2018), https://www.msnbc.com/msnbc/watch/privacy-is-a-human-right-apple-ceo-tim-cook-1197152323753?v=railb& [https://perma.cc/PR3V-K777] ("[Data] privacy . . . is a human right, it's a civil liberty . . . like freedom of speech and freedom of the press."); *see also* Rachel Lerman, *Data Privacy Is a Human Right, Microsoft CEO Satya Nadella Says*, STUFF (May 8, 2018) https://www.stuff.co.nz/technology/digital-living/103709739/data-privacy-is-a-human-right-microsoft-ceo-satya-nadella-says [https://perma.cc/N3FM-78R2] ("[Microsoft's CEO] praised the [GDPR], calling [data] privacy a human right.").

[17] *See, e.g.*, Brian Naylor, *Firms Are Buying, Sharing Your Online Info. What Can You Do About It?*, NPR (July 11, 2016), https://www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it [https://perma.cc/376P-JBNT]; Steve Poreca, *How Big Data Shows Big Results with Spotify*, NE. U. LEVEL (Apr. 27, 2018), https://www.northeastern.edu/levelblog/2018/04/27/big-data-shows-big-results-spotify/ [https://perma.cc/TXD6-VT8N]; Mark van Rijmenam, *What Data Do the Five Largest Tech Companies Collect — Infographic*, DATAFLOQ (July 16, 2013), https://datafloq.com/read/what-data-do-the-five-largest-tech-companies-colle/427 [https://perma.cc/HYY5-6PYV].

likely users of their own technology, it would be incredibly hard for these CEOs to deny the "human" element of the data they knowingly process and to deny the implications of not managing that information carefully.

Companies that deal in data have had to react to this changing mindset—some responding more successfully than others. On the first effective day of the GDPR, both Facebook and Google were accused of violations, including requiring users to consent to targeted advertising to use the services as well as unnecessarily collecting data.[18] Prior to these alleged violations, Facebook CEO Mark Zuckerberg had stated that Facebook would be ready to comply by the time the GDPR took effect.[19]

Some companies, however, have responded favorably to the changing law and policy in the data privacy arena. When the retail giant Target was hacked in 2013 and had millions of customers' credit card information stolen, the company responded in the following months with a variety of data security measures, including practical support for affected customers (e.g. discounts, credit monitoring, etc.), an overhaul of its security systems, and additional employee training in how to protect customers' sensitive information.[20] In addition, Uber has taken a strong position on data privacy by terminating an in-house attorney and security officer who covered up evidence of a data breach and failed to comply with legal reporting obligations.[21]

---

[18] *See* Chris Foxx, *Google and Facebook Accused of Breaking GDPR Laws*, BBC (May 25, 2018), https://www.bbc.com/news/technology-44252327 [https://perma.cc/YTX7-EPKL]; *see also* Novak, *supra* note 6.

[19] *See* Novak, *supra* note 6.

[20] Eric Dezenhall, *A Look Back at the Target Breach*, HUFFINGTON POST (Apr. 6, 2015), https://www.huffingtonpost.com/eric-dezenhall/a-look-back-at-the-target_b_7000816.html [https://perma.cc/GRP4-QCQJ] (last updated June 6, 2015).

[21] Lorelei Laird, *Uber Ousts In-House Counsel Who Suppressed Information About 2016 Data Breach*, ABA J. (Nov. 22, 2017), http://www.abajournal.com/news/article/uber_ousts_in_house_counsel_who_suppressed_information_about_2016_data_brea [https://perma.cc/LMH6-TPRZ].

CEOs, as the managers and strategic heads of these companies, wield incredible power and influence,[22] extending to the treatment of data privacy concerns and compliance with laws protecting data privacy rights. The need for sound corporate strategies to successfully adhere to the growing number of data privacy regulations should be paramount to the CEO of any data-managing company. CEOs are currently insulated from personal liability by most corporate law regimes. Although companies themselves may be liable for breaching data privacy laws, this Note will suggest that directors should be personally liable at the highest international levels for severe missteps in data privacy protection. After all, if data privacy is now considered a human right—as recognized by many corporate officers themselves—the world is substantially less likely to be forgiving.[23]

A. The Current State of Corporate Data Privacy Obligations

This Note considers how three different systems—the EU, the United States, and the UN—protect data privacy rights. All three systems tackle protection of data rights differently, and the penalties they assess range from small-scale injunctive measures to billions of dollars in fines.[24] In all of

[22] *See* Z. Jill Barclift, *Corporate Governance and CEO Dominance*, 50 WASHBURN L.J. 611, 616 (2011).

[23] *See* Sarah St. Vincent, *Data Privacy Is a Human Right. Europe Is Moving Toward Recognizing That.*, FOREIGN POL'Y IN FOCUS (Apr. 19, 2018), https://fpif.org/data-privacy-is-a-human-right-europe-is-moving-toward-recognizing-that/ [https://perma.cc/YPS9-ZQ5Z]; *see also* James Nickel, *Human Rights*, STAN. ENCYCLOPEDIA PHIL. ARCHIVE (Feb. 7, 2003), https://plato.stanford.edu/archives/spr2017/entries/rights-human/ [https://perma.cc/E97P-UVKH] (last updated Nov. 8, 2014) ("Human rights declarations and treaties are intended to change existing norms, not just describe the existing moral consensus.").

[24] *See Fines and Penalties*, GDPREU.ORG, https://www.gdpreu.org/compliance/fines-and-penalties/ [https://perma.cc/UX9Q-APKG]; *see also* Ieuan Jolly, *Data Protection in the United States: Overview*, THOMSON REUTERS PRAC. L., Oct. 1, 2018, https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&first

these regimes, however, particular focus is placed on the obligations that companies have in maintaining users' data privacy.[25] Another commonality among the systems is that the strongest data privacy regulations exist only at the national or regional level.[26]

A key enforcement issue for each set of policies is the lack of truly international oversight; this is especially true as the lines between government and the private sector blur due to government reliance on the private sector for data processing and collection.[27] There is no strong international voice providing guidance on penalties for misappropriation of sensitive data, leaving open a gap that an international organization like the United Nations should fill.

1. The European Union Approach

In May 2018, the GDPR[28] came into effect in the EU, replacing the Data Protection Directive (95/46/EC) of 1995, as

Page=true&comp=pluk&bhcp=1 (on file with the *Columbia Business Law Review*).

[25] *See* Jolly, *supra* note 24.

[26] *See generally GDPR Overview*, *supra* note 7; *see also* Jolly, *supra* note 24; Deborah Thoren-Peden & Catherine Meyer, *USA: Data Protection 2018*, INT'L COMP. L. GUIDES (Dec. 6, 2018), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa#chaptercontent1 [https://perma.cc/2CE5-VBJ8]. For an example of a state statute, see CAL. BUS. & PROF. CODE § 22575 (West 2019).

[27] PRIVACY INT'L, THE KEYS TO DATA PROTECTION 5 (2018), https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf [https://perma.cc/SQB4-CR86] ("There is often little or no public consultation, transparency of resource-allocation, and oversight or audits of how these systems are functioning. Additionally, governments are increasingly relying on industry to deploy systems and run software; equally, industry are becoming dependent on governments sanctioning access to data. In this way, the separation between government and industry will blur, and this will fuse their respective duties and obligations.").

[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119) 1.

a comprehensive attempt to protect EU citizens' data rights. It carries heavy penalties for any data holder or processor who abuses citizens' data.[29] The GDPR factors in the seriousness of a company's effort to comply with the requirements in determining the magnitude of the fine.[30] Violations of its requirements can include a fine of up to €20 million (approximately $22.5 million as of this writing), or four percent of a company's worldwide annual revenue of the prior financial year, whichever is higher.[31]

When the European Commission announced its plan to overhaul the GDPR's predecessor, it put particular emphasis on increasing the "responsibility and accountability" of companies engaged in data processing both in the EU and abroad.[32] The personal data intended to be covered by the regulation was broad, including anything from a person's name to their IP address to their comprehensive medical records.[33] The GDPR, as passed, achieved this initial goal of the Commission by protecting expansive categories of

[29] *See* Ivan Klekovic, *EU GDPR vs. European Data Protection Directive*, EU GDPR ACAD.: EU GDPR BLOG (Oct. 30, 2017), https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/ [https://perma.cc/V24L-XV2Z] (discussing the main changes brought upon by the GDPR, including an expansion of what is considered personal information in the digital world, higher burdens on data processors, an expansion of extra-territorial obligations on EU based processors and controllers, and significantly higher fines for violations); *see also GDPR Overview*, *supra* note 7.

[30] *See* Danny Palmer, *What Is GDPR? Everything You Need to Know About the New General Data Protection Regulations*, ZDNET (May 23, 2018), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/ [https://perma.cc/9A5A-VB34] ("[GDPR] [f]ines will depend on the severity of the breach and on whether the company is deemed to have taken compliance and regulations around security in a serious enough manner.").

[31] *Fines and Penalties*, *supra* note 24.

[32] *See* European Commission Press Release IP/12/46, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.htm [https://perma.cc/46LE-Z6KG].

[33] *See id.*

personal data as outlined in Articles 4(1) and 9(1).[34] This wide range of protected types of data, however, mainly places substantial pressure on companies to make sure that they are getting the "freely given, specific, informed and unambiguous" consent of their users for the various types of data they may collect, store or process for them.[35]

In addition to being inclusive in the types of data it protects, the GDPR is also equally inclusive in the parties that are subject to its regulations. The GDPR "not only applies to organisations located within the EU but also applies to organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects."[36] Moreover, the GDPR is applicable to "all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location."[37]

The GDPR requires companies to obtain user consent if they intend to use a person's sensitive data.[38] The conditions for consent "must be given in an intelligible and easily

[34] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), arts. 4, 9, 2016 O.J. (L 119) 1, 33–35, 38–39. Data can include a number of different identifiers, "such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." *Id.* at art. 4(1). In addition, the GDPR states:

> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Id. at art. 9(1).

[35] *Id.* at art. 4(11).

[36] *GDPR FAQs*, EUGDPR.ORG, https://eugdpr.org/the-regulation/gdpr-faqs/ [https://perma.cc/HCK5-937Z].

[37] *Id.*

[38] *See id.*

accessible form, with the purpose for data processing attached to that consent, meaning it must be unambiguous."[39] Individuals must also be able to easily withdraw this consent.[40] Overall, these provisions make for some of the strictest regulations on data privacy currently in existence.

2. The United States Approach

U.S. companies are also subject to a host of laws and regulations protecting data privacy.[41] There are laws at both the federal and state levels, with the federal laws focusing primarily on industry sector regulation and the state laws focusing more on protecting individuals' personal information from misappropriation.[42] However, the varying levels of protection provided by different states can make it difficult for companies to know what levels of protection apply to them.[43] For example, a company that processes data in both the United States and the European Union would be subject to two differing levels of protection, as the GDPR is more comprehensive than similar regulations in the United States.[44] And due to the breadth of the GDPR's

[39] *Id.*

[40] *See id.*

[41] *See* Thoren-Peden & Meyer, *supra* note 26; *see also* Eric Vanderburg, *Information Security Compliance: Which Regulations Relate to Me?*, TCDI BLOG, https://www.tcdi.com/information-security-compliance-which-regulations/ [https://perma.cc/4Q2G-P2XK]; Stuart Tarmy, *Healthcare Companies Struggle to Comply with GDPR Data Privacy Regulations*, DATAVERSITY (Mar. 26, 2018), https://www.dataversity.net/healthcare-companies-struggle-comply-gdpr-data-privacy-regulations/ [https://perma.cc/5R6Y-8FX8].

[42] *See* Thoren-Peden & Meyer, *supra* note 26.

[43] *See generally Data Security Laws: Private Sector*, NAT'L CONF. ST. LEGISLATURES (Jan. 4, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx [https://perma.cc/9MYU-RS2K].

[44] *See* Derek Hawkins, *The Cybersecurity 202: Why a Privacy Law Like GDPR Would Be a Tough Sell in the U.S.*, WASH. POST (May 25, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07

extraterritorial reach, that same company could be held liable for processing an EU user's data in the United States if it does not comply with GDPR requirements.[45] This problem, which can be confusing for companies and increase the likelihood of data privacy violations, highlights the need for a standard level of protection and a centralized authority to evaluate purported violations.

Penalties for violations of U.S. data privacy laws can be civil and/or criminal, and involve remedies such as fines, injunctions, and varying criminal penalties.[46] Examples of U.S. federal laws protecting data privacy include the Gramm Leach Bliley Act, the Health Information Portability and Accountability Act and the Telephone Consumer Protection Act.[47] Additionally, laws like Massachusetts's 201 CMR 1700 and the California Consumer Privacy Act of 2018 protect data on a state level.[48] The fines for violations of these laws tend to be connected to the number of infractions and vary in the amount of financial penalties per violation.[49] The FTC, one of the main enforcement agencies, draws its power from section 5 of the Federal Trade Commission Act, which prohibits

e83/?utm_term=.148d6642a95e [https://perma.cc/4Z8P-QRFY]; *see also Europe's Tough New Data-Protection Law*, ECONOMIST (Apr. 5, 2018), https://www.economist.com/business/2018/04/05/europes-tough-new-data-protection-law [https://perma.cc/9UTU-ANFG].

45 *See* Hawkins, *supra* note 44.

46 *See* Thoren-Peden & Meyer, *supra* note 26.

47 *See* Gramm–Leach–Bliley Act, Pub. L. No. 106-102, § 103, 113 Stat. 1338, 1343 (1999) ("[E]fficiently deliver information and services that are financial in nature through the use of technological means, including any application necessary to protect the security or efficacy of systems for the transmission of data or financial transactions[.]"); *id.* § 501 ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."); *see also* Telephone Consumer Protection Act, 47 U.S.C. § 227 (2012); Other Requirements Relating to Uses and Disclosures of Protected Health Information, 45 C.F.R. § 164.514 (2019).

48 *See* Thoren-Peden & Meyer, *supra* note 26; *see also* CAL. CIV. CODE §§ 1798.100–.199 (West 2019) (effective Jan. 1, 2020); 201 MASS. CODE REGS. 17 (2009).

49 *See* Thoren-Peden & Meyer, *supra* note 26.

"unfair or deceptive acts or practices in or affecting commerce."[50] Both the Federal Trade Commission ("FTC") and the Department of Health and Human Services ("DHHS"), another common enforcement agency, have assigned millions of dollars in penalties to companies violating federal data privacy laws.[51]

The U.S. regime differs from the EU's GDPR, which holds companies liable based on the severity of the infraction without assigning each individual infraction a monetary value.[52] However, the key difference between the two regimes is that "the United States does not frame data privacy as a fundamental right." and "[n]either the U.S. Constitution nor the Bill of Rights mentions 'privacy.' Nonetheless, an interpreted right to privacy has emerged in constitutional jurisprudence."[53] This divergence between the two jurisdictions on the fundamental nature of the right to privacy is likely related to the substantially smaller liability the

[50] Margaret Byrne Sedgewick, *Transborder Data Privacy as Trade*, 105 CALIF. L. REV. 1513, 1523 (2017) ("Since 2002, the FTC has brought approximately 100 actions against companies to protect millions of consumers from deceptive and unfair data practices. Under the unfairness prong, the FTC pursues businesses for practices that 'cause substantial injury to consumers which is not reasonably avoidable by consumers themselves' and not 'outweighed by countervailing benefits to consumers or to competition.'") (citing Federal Trade Commission Act, 15 U.S.C. § 45(n) (2012)); *see also* Julie Brill, Former Comm'r, Fed. Trade Comm'n, Global Regulation of Data Flows in a Post-Snowden World — Killingstad Global Insights Lecture at the Tuck School of Business, Dartmouth College (Feb. 18, 2015), (transcript available at https://www.ftc.gov/public-statements/2015/02/global-regulation-data-flows-post-snowden-world-killingstad-global [https://perma.cc/KVK8-7ML5]).

[51] *See* Thoren-Peden & Meyer, *supra* note 26; Press Release, U.S. Dep't of Health & Human Servs., Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History (Oct. 15, 2018), https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html [https://perma.cc/M3PG-HHH6].

[52] *See Fines and Penalties*, *supra* note 24.

[53] Sedgewick, *supra* note 50, at 1522.

United States imposes for data privacy violations as compared to the EU.[54]

3. The United Nations Approach

Finally, the U.N. recognizes data privacy rights, but it deals with state actors' obligations and not private corporate obligations. In 1988, the Office of the High Commissioner for Human Rights issued CCPR General Comment No. 16, which indicates that member states have an obligation to protect every person from "arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour and reputation," including personal data stored on computers or data banks.[55] This Comment also recognized the shift from thinking of data privacy as a purely privacy-centered right to a specific type of human right.[56]

In many ways, the U.N.'s approach to data privacy is stronger than that of countries like the United States because it explicitly ties data privacy rights to the general right to privacy.[57] The U.N. General Assembly approved a resolution calling on member states to take actions to address violations of data privacy and to update their national legislation accordingly.[58] Of particular interest is the U.N.'s request for member states to create national oversight bodies to monitor for data privacy violations.[59] As discussed in Part III.B, the current regulatory regimes overseeing data privacy rights reinforce the notion that data is a modern utility and should be regulated accordingly.

---

[54] *See* David Meyer, *In the Wake of GDPR, Will the U.S. Embrace Data Privacy?*, FORTUNE (Nov. 29, 2018), http://fortune.com/2018/11/29/federal-data-privacy-law/ [https://perma.cc/HS24-HG5Q].

[55] Office of the High Comm'r for Human Rights, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation on its Thirty-Second Session ¶¶ 1, 10 (Apr. 8, 1994).

[56] *See id.*; *see also* Diggelmann & Cleis, *supra* note 9.

[57] *See* G.A. Res. 68/167 (Dec. 18, 2013).

[58] *Id.* ¶ 4.

[59] *Id.*

The U.N. has not addressed private actors' violations of individuals right to data privacy, primarily because the U.N. was not created with the intention of dealing with non-state actors.[60] But this does not mean that it is impossible to create such a system. A framework already exists for imposing sanctions on state actors, including serious sanctions for gross human rights violations.[61] In principle, this framework could be extended to cover the violation of data privacy rights by non-state actors.

III. ISSUES IN APPLICATION OF SANCTIONS ON PRIVATE, CORPORATE OFFICERS

The fines, both threatened and imposed, on companies by laws and regulations like the GDPR may not effectively alter corporate actions to the extent intended.[62] While existing data privacy regimes attempt to deter data privacy violations, the main issue is that the mega, data-driven companies like Google and Facebook earn exceedingly high revenues that current fines, even at the higher end of the range, do not dent corporate coffers enough to create the deterrent effect for which they were designed.[63] While it is true that "[i]n addition to civil and criminal sanctions, security breaches can have far reaching consequences for companies in terms of loss of

[60] *See* Noah Birkhäuser, Sanctions of the Security Council Against Individuals – Some Human Rights Problems (May 2005) (unpublished manuscript), http://esil-sedi.eu/wp-content/uploads/2018/04/Birkhauser.pdf [https://perma.cc/3U7K-G4YN].

[61] *See UN Sanctions: What They Are, How They Work, and Who Uses Them*, UN NEWS (May 4, 2016) [hereinafter *UN Sanctions*], https://news.un.org/en/story/2016/05/528382-un-sanctions-what-they-are-how-they-work-and-who-uses-them [https://perma.cc/PA7Z-BDGF].

[62] *See* Matt Novak, *Facebook Fined Just $645,000 in UK Over Cambridge Analytica Scandal, Money It Makes in Less Than 10 Minutes*, GIZMODO (Oct. 25, 2018), https://gizmodo.com/facebook-fined-just-645-000-in-uk-over-cambridge-analy-1829989116 [https://perma.cc/3U2T-XXU8].

[63] *See id.* ("Facebook has been fined £500,000 ($645,000) by the United Kingdom . . . over the Cambridge Analytica scandal. The miniscule fine was the most allowed under the law, but Facebook can probably find that kind of money in its couch cushions. Based on last year's revenue, Facebook makes $645,000 in less than 9 minutes of operation.").

customer confidence and trust, customer churn, and loss of revenue, market share, brand and shareholder value," the reliance many consumers have on data driven companies like Google and Facebook may dilute the response from corporate officers in dealing with data privacy violations.[64]

A. Sanctions are Historically Targeted at Government Agents

In general, sanctions—as outlined in Chapter VII of the U.N.'s Charter—are a tool used to enforce compliance with international laws and U.N. standards or to punish extreme actions.[65] The U.N. Security Council hands down these sanctions, and they have taken a number of forms, including "comprehensive economic and trade sanctions" and "more targeted measures such as arms embargoes, travel bans, and financial or commodity restrictions."[66]

There is no procedure for an individual to petition the U.N. Security Council if they are sanctioned. Currently, only states may appear before the U.N. Security Council to challenge the sanctions or attempt to show that they have resolved the issues that led to the sanction.[67] This could raise serious issues in the data privacy space if a CEO or other corporate officer was targeted by an international sanction, as he or she might not be able to show on an individual basis that the company had become compliant with U.N. standards in order to get the sanction lifted. Rule 37 of the Provisional Rules of Procedure of the U.N. Security Council provides that the U.N. Security Council can only allow member states to appear before the Council and, although the states may invite others to supply additional information, there is no provision that would allow an individual to appear to discuss an issue that

64 *See* Jolly, *supra* note 24.

65 *See, e.g.*, U.N. Charter arts. 39, 41.

66 *Sanctions*, UNITED NATIONS SECURITY COUNCIL, https://www.un.org/securitycouncil/sanctions/information [https://perma.cc/5SX2-ND4F].

67 *See* Birkhäuser, *supra* note 60, at 2 n.7.

addresses only themselves.[68] This means a corporate officer would not only have to appear before the Council as the guest of a member state, but he or she may still be unable to address the Council if the issue raised concerns only a personal, not national, problem.[69]

As individuals are not permitted to go before the Security Council in matters concerning themselves, U.N. member states alone must uphold sanctions against them.[70] This can be problematic if a state chooses to ignore the mandate of the Security Council. Even if a private sanction existed under U.N. regulations, corporations that have the bulk of their assets in a certain country may be able to avoid the full force of a sanction if that country refuses to enforce the sanction.[71] In other words, sanctions cannot be weaponized or used as a deterrent unless they are enforced by the member state.[72] Although the U.N. retains the ability to garner agreements from member states to enforce Security Council sanctions and may call upon member states to honor those agreements,

[68] *Id.* at 2 n.7. *See generally* United Nations Security Council Provisional Rules of Procedure 37, 39, https://www.un.org/securitycouncil/content/rop/chapter-6 [https://perma.cc/DV28-URHC].

[69] *See* Birkhäuser, *supra* note 60, at 2–3.

[70] *See id.* at 2.

[71] *See generally* Benjamin Alter, *Sanctions Are Congress's Path Back to Foreign Policy Relevance*, LAWFARE (Mar. 27, 2018), https://www.lawfareblog.com/sanctions-are-congresss-path-back-foreign-policy-relevance [https://perma.cc/J3R3-MW86]; *see also* Robbie Gramer & Dan de Luce, *State Department Scraps Sanctions Office*, FOREIGN POL'Y (Oct. 26, 2017), https://foreignpolicy.com/2017/10/26/state-department-scraps-sanctions-office/ [https://perma.cc/5AQQ-D4W9]; James A. Paul & Senwan Akhtar, *Sanctions: An Analysis*, GLOBAL POL'Y F. (Aug. 1998), https://www.globalpolicy.org/security-council/index-of-countries-on-the-security-council-agenda/sanctions/41612-sanctions-an-analysis.html [https://perma.cc/3K8W-S8VV].

[72] *See generally* Frederic L. Kirgis, *Enforcing International Law*, AM. SOC'Y INT'L L. (Jan. 22, 1996), https://www.asil.org/insights/volume/1/issue/1/enforcing-international-law [https://perma.cc/SZ4V-JVQ2]; *see also* Meetings Coverage, Security Council, Full Support of Member States Key to Effective Sanctions Regimes, Assistant Secretary-General Tells Security Council, U.N. Doc. SC/12941 (Aug. 3, 2017), https://www.un.org/press/en/2017/sc12941.doc.htm [https://perma.cc/7L82-AB7L].

sanction enforcement has historically fallen to the discretion of the individual state.[73] Because these sanctions have historically targeted member states and government actors,[74] it may be useful to frame data and tech CEOs as agents of companies that serve a purpose similar to that of a public utility when generating future compliance guidelines.

Sanctioning of private individuals for human rights violations has received some traction in recent years, notably with the passage of the Global Magnitsky Human Rights Accountability Act in the United States.[75] Under this Act, the President of the United States has the power to sanction individuals, including private actors, for human rights abuses.[76] These sanctions can include a host of tactics such as visa blockages, asset freezes, and prohibitions on transacting with U.S. businesses and banks.[77]

B. The Role of Data-Driven Companies as Utilities

Today**,** communication primarily occurs through data, supplanting utilities like telephone services in importance.[78] Because of this, what constitutes a utility under a traditional framework should be reexamined. Companies like Facebook, Google, and Amazon not only highlight the extent to which data-driven companies have become ingrained in society, but they also provide insight into the new ways in which global

[73] *See* Kirgis, *supra* note 72.

[74] *See generally* Birkhäuser, *supra* note 60.

[75] Global Magnitsky Human Rights Accountability Act, Pub L. No. 114-328, 130 Stat. 2533 (2016).

[76] *Id.* § 1263(a)(1).

[77] Id. at § 1263(b). *See generally The US Global Magnitsky Act: Questions and Answers*, HUM. RTS. WATCH (Sept. 13, 2017), https://www.hrw.org/news/2017/09/13/us-global-magnitsky-act [https://perma.cc/X5WC-PPDT].

[78] *See generally* Larry Alton, *Phone Calls, Texts or Email? Here's How Millennials Prefer to Communicate*, FORBES (May 11, 2017), https://www.forbes.com/sites/larryalton/2017/05/11/how-do-millennials-prefer-to-communicate/#6a83fc596d6f [https://perma.cc/RQG9-SY7K]; *see also* Frank Newport, *The New Era of Communication Among Americans*, GALLUP (Nov. 10, 2014), https://news.gallup.com/poll/179288/new-era-communication-americans.aspx [https://perma.cc/UF4V-63Y2].

communication primarily occurs.[79] Historically, communication was only possible through postal mail or via telephones and telegraphs, but with the advent of satellites and advancements in computing and data processing, global communication can occur virtually instantaneously with applications like Apple's FaceTime, Skype, Google Talk, or any number of other applications that share data between users.[80] Just as traditional forms of communication were regulated as utilities, the next generation of regulations may similarly target the realm of data-driven communication as a modern utility.

However, defining these services as utilities is difficult, because the term "utility" itself is ambiguous. When attempting to define a utility, "[m]ost descriptions of the concept are circular: a utility is a company, such as a telephone network, water, or electricity provider, which has special obligations because it functions as a public utility."[81] Social media and data-driven companies have so far appeared to defy this definition for a multitude of reasons, including their constant displacement of one another, their lack of connection with other utilities' essentiality of "survival, economic success, or online life," and the fact that people could go their entire lives without ever using their services.[82]

[79] *See generally* Vineet Kaul, *The Changing World of Media & Communication*, 2 J. MASS COMM. & JOURNALISM 116 (2012).

[80] *See* Vineet Kaul, *The Digital Communications Revolution*, 2 ONLINE J. COMM. & MEDIA TECHNOLOGIES, July 2012, at 113, 114–15, http://www.ojcmt.net/download/the-digital-communications-revolution.pdf [https://perma.cc/9GEN-9BR2]; *see also Social Networking Provides Instantaneous Communication Worldwide*, BBG COMM. (Dec. 11, 2012), http://www.bbgcommunicationscorp.com/social-network-innovations/article/10.php [https://perma.cc/G368-W584].

[81] Kevin Werbach, *The Network Utility*, 60 DUKE L.J. 1761, 1788 n.126 (2011) ("A public utility is a business that furnishes an everyday necessity to the public at large. Public utilities provide water, electricity, natural gas, telephone service, and other essentials.") (citing WEST'S ENCYCLOPEDIA OF AMERICAN LAW 173 (2d ed. 1998)).

[82] Adam Thierer, *The Perils of Classifying Social Media Platforms as Public Utilities*, 21 J. COMM. L. & TECH. POL'Y 249, 277 (2013).

As a result, while telephones and postal mail are regulated as utilities in many parts of the world,[83] the same cannot be said of more modern forms of communication. In the United States, the Federal Communications Commission ("FCC") regulates wireless communication, but not to the same degree as wired communication or other more tangible utilities like water or electricity.[84] Regulating utilities generally deals with the managing of natural monopolies to ensure adequate and safe distribution.[85] With most communication happening through wireless mediums now, it makes sense to begin regulating this form of communication more heavily to protect users' interests.

There is concern that regulation of the internet and wireless communication on a level similar to water and electricity could stifle competition and innovation in these spaces.[86] However, if the regulations were targeted at protecting the key, narrow interest of data privacy, it may be possible to minimize any disruption to competition or innovation.[87] By focusing less on prices or the availability of the "utility" and instead on protective measures aimed at preventing data misappropriation, it may be possible to regulate utilities in a way that is as modern as the utility

[83] *See What We Do*, FED. COMM. COMMISSION, https://www.fcc.gov/about-fcc/what-we-do [https://perma.cc/U68D-GLVG]; *About the Postal Regulatory Commission*, POSTAL REG. COMMISSION, https://www.prc.gov/about [https://perma.cc/82V7-MDHR].

[84] *See* Joe Harpaz, *The Internet: Commodity or Utility?*, FORBES (Jan. 27, 2015), https://www.forbes.com/sites/joeharpaz/2015/01/27/the-internet-commodity-or-utility/#694af84f6eff [https://perma.cc/UUN6-964V].

[85] *See* Sean Ross, *How Strongly Does Government Regulation Impact the Utilities Sector?*, INVESTOPEDIA (July 9, 2015), https://www.investopedia.com/ask/answers/070915/how-strongly-does-government-regulation-impact-utilities-sector.asp [https://perma.cc/T6RB-4E73].

[86] *See id.*

[87] *See generally* Thierer, *supra* note 82, at 251; *see also* Mark Newton Lowry & Lawrence Kaufman, *Performance-Based Regulation of Utilities*, 23 ENERGY L.J. 399, 426 (2002).

itself.[88] An additional concern is that regulation can often open an industry to political influence, as regulations are handled by agencies with heads appointed by the governing political party.[89] As a result, the regulation of an industry as a public utility often transforms the industry into one that is controlled by interested parties.[90] In the case of data-driven companies and social media agents, classifying them as utilities and allowing interest groups to take control and entrench themselves as regulators may do more harm than good, as their interests may not align with the need for increased data privacy and regulation.

In addition, a key question here is who should do the regulating? As addressed in Part IV, the regulators will need international reach, because data can be spread across the globe faster than the blink of an eye. Regulating data in one country would not be enough to rein in data-driven companies who operate globally—at least not in a way that would pressure their executives to take truly substantive measures to change their data-protection policies.

Whether these data companies are actually considered utilities under traditional standards remains unclear.[91] However, the need to implement stronger regulations that prevent data breaches or data misappropriation by companies maintaining user data is clear.[92] Without a stronger protection regime with heavier penalties, it is unlikely that these critical data resources will receive the protection they

88 *See* Thierer, *supra* note 82, at 288–89; *see also* Newton & Kaufman, note 87, at 426.

89 *See* Thierer, *supra* note 82, at 272–73.

90 *See id*. at 271–72 (discussing "capture theory" in utility regulation and its detrimental effects on consumers and the industry as a whole).

91 *See* Catherine Andrews, *Data-As-a-Utility: A New Era for the Public Sector*, GOVLOOP (Aug. 25, 2015), https://www.govloop.com/resources/data-as-a-utility-a-new-era-for-the-public-sector/ [https://perma.cc/623B-7PDQ]; *see also* Mark A. Jamison, *Should Google Be Regulated as a Public Utility?*, 9 J.L., ECON. & POL'Y 223, 231–34 (2013).

92 *See* Adam Schwartz, *You Should Have the Right to Sue Companies That Violate Your Privacy*, ELECTRONIC FRONTIER FOUND. (Jan. 7, 2019), https://www.eff.org/deeplinks/2019/01/you-should-have-right-sue-companies-violate-your-privacy [https://perma.cc/3U8V-NRKL].

require.[93] While classifying data companies as social utilities may not be the best course of action, regulating these companies to a higher degree certainly is. Just as the heads of historically regulated utilities and the companies that functioned within them were held responsible for critical failures, the new generation of leaders within the data realm should likewise face accountability when they fail.[94] Because the nature of these failures is often global in scope, the regulation and accountability regime for addressing shortcomings should be proportionate.

IV. CREATING A SANCTION ESTABLISHING PERSONAL LIABILITY AND APPLYING IT

Creating a sanction that allows the U.N. Security Council to target corporate officers—primarily CEOs—for data privacy violations and enforce such a sanction is necessary to more effectively deter future data privacy violations on an international scale. Businesses that deal heavily with personal data and are knowing violators of international data privacy laws need a deterrent that moves beyond corporate fines and instead focuses on corporate officers as individuals. Companies like Facebook, Apple, and Microsoft all have prominent leaders with unparalleled influence over their companies' compliance with data privacy laws.[95] These leaders recognize the need for strong data privacy laws, and many recognize data privacy as a human right, however there is evidence that violations may still occur even in the face of

[93] *See* Michael M. O'Hear, *Sentencing the Green-Collar Offender: Punishment, Culpability, and Environmental Crime*, 95 J. CRIM. L. & CRIMINOLOGY 133, 145 (2004); *see also* Keith Johnson, *What Is Consumer Data Privacy, and Where Is It Headed?*, FORBES (July 9, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/07/09/what-is-consumer-data-privacy-and-where-is-it-headed/#3828a0741bc1 [https://perma.cc/98YY-2R5K].

[94] *See* O'Hear, *supra* note 93, at 141–46.

[95] Cecilia Kang, *Tech Industry Pursues a Federal Privacy Law, on Its Own Terms*, N.Y. TIMES (Aug. 26, 2018), https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html [https://perma.cc/L4M8-2MDR].

financial penalties.[96] By utilizing the world's most internationally recognized legal body, the UN, it may be possible to hold corporate officers accountable for data privacy violations via the human rights framework.

A. Wading into the Private Sector

Many countries favor the U.N. playing an enlarged role in promoting human rights internationally.[97] As discussed in Part II, data privacy is often now viewed more as a human right than a basic privacy right. With that particular distinction comes a heightened international scrutiny due to the sensitive nature of issues that often arise involving human rights. With a well-established framework for sanctioning state actors for violations of human rights, the extension of sanctions to private actors for severe data privacy violations that rise to the level of a human rights violations is not implausible. This is especially true when one considers that the companies these private actors lead could eventually be regarded as publicly regulated utilities.[98]

1. Current U.N. Security Council Sanctions Framework

As previously discussed, the U.N. Security Council has the power to issue sanctions in response to human rights violations. The U.N. Security Council, comprised of representatives from fifteen countries, may issue sanctions against states or state actors, subject to the veto power of the

[96] *See* James Sanders & Dan Patterson, *Facebook Data Privacy Scandal: A Cheat Sheet*, TECHREPUBLIC (Dec. 11, 2018), https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/ [https://perma.cc/9RCD-4JG3] (detailing the history of Facebook's data privacy violations).

[97] In an international poll of select U.N. member states, an average of seventy percent of respondents per state favored the U.N. promoting human rights in member states, and majorities in most polled countries also favored the U.N. doing more than it currently is to achieve human rights objectives. COUNCIL ON FOREIGN RELATIONS, PUBLIC OPINION ON GLOBAL 87–88 ISSUES (2009).

[98] *See infra* Section III.B.

Council's five permanent members.[99] The United States, Russia, China, France, and the United Kingdom all hold veto powers over sanctions,[100] and it is possible that they would prohibit sanctions targeting their own citizens for data privacy violations, a problem that is addressed in Section IV.A.3.

Sanctions, supposedly a "last resort," are so powerful on the international stage that the mere hint of them can induce the targeted party to begin to act.[101] If the threat of sanctions does not work, the Council typically passes a resolution indicating who will be sanctioned and what those sanctions will entail.[102] It can also set up a sanctions committee "to implement, monitor and provide recommendations to the Council on particular sanctions regimes," pursuant to its Article 29 powers.[103] Expert panels may also be implemented to assist the sanction committee in monitoring compliance and provide feedback to either the sanctions committee or the Council directly.[104] These expert panels may be the best way

[99] *See Functions and Powers*, UNITED NATIONS SECURITY COUNCIL, https://www.un.org/securitycouncil/content/functions-and-powers [https://perma.cc/6ZU9-L3XK]; *see also Voting System*, UNITED NATIONS SECURITY COUNCIL, https://www.un.org/securitycouncil/content/voting-system [https://perma.cc/XN5H-FMB2]. There are fifteen total members on the Security Council, with five seats permanently filled by China, France, the Russian Federation, the United Kingdom, and the United States; the other ten seats are comprised of members elected for two-year terms by the general assembly. *Current Members*, UNITED NATIONS SECURITY COUNCIL, https://www.un.org/securitycouncil/content/current-members [https://perma.cc/WMF8-LBSY]. Non-members can contribute to Security Council discussions, but they do not have a vote. *Id.*

[100] *See* Press Release, General Assembly, Member States Call for Removing Veto Power, Expanding Security Council to Include New Permanent Seats, as General Assembly Debates Reform Plans for 15-Member Organ, U.N. Press Release GA/12091 (Nov. 20, 2018) [hereinafter Call for Removing Veto Power], https://www.un.org/press/en/2018/ga12091.doc.htm [https://perma.cc/NG3A-5QBU].

[101] *See UN Sanctions, supra* note 61.

[102] *Id.*

[103] *Id.*

[104] *Id.* ("An expert panel monitors the implementation of the sanctions measures and reports its findings to the committee, or in some cases directly

to address sanctions for data privacy violations against corporate officers, not only because the field of data processing is complex, but also because individuals lack standing to appear before the U.N. Security Council. These expert committees could meet with sanctioned corporate officers to monitor their compliance and recommend the Council lift the sanctions once compliance is confirmed.

However, even after a sanction is issued, the Security Council relies on the members of the United Nations for the implementation and execution of its sanctions.[105] This is often difficult due to the limited resources and limited political incentive that many nations have.[106] However, in the case of asset freezes or travel bans—which would be most applicable to corporate executives—the cost of enforcement would likely be low. Moreover, because most people who access technological services are exposed to data privacy issues, and almost every country has citizens who access this technology, there is an inherent political incentive to prevent the exploitation of a country's own citizens.[107]

2. The Process for Establishing Authority

Knowing that the framework for holding individuals accountable via U.N. sanctions exists, the next step is amending the U.N. Charter to allow the Security Council to target private individuals. This process is incredibly

to the Council. Expert panels are usually comprised of between five to eight technical experts, all of whom are appointed by the Secretary-General. Expertise in these panels depends on the sanctions imposed, but may include . . . human rights/humanitarian experts."); *see also* U.N. Charter art. 29 ("The Security Council may establish such subsidiary organs as it deems necessary for the performance of its functions.").

105 Jonathan Masters, *What Are Economic Sanctions?*, COUNCIL ON FOREIGN REL. (Aug. 7, 2017), https://www.cfr.org/backgrounder/what-are-economic-sanctions [https://perma.cc/U8MB-SCKF].

106 *Id.*

107 Hannah Ritchie, *How Many Internet Users Does Each Country Have?*, OUR WORLD IN DATA (Jan. 22, 2019), https://ourworldindata.org/how-many-internet-users-does-each-country-have [https://perma.cc/FZ9J-B4W2].

challenging,[108] but if the initial alteration is limited enough in scope, it is possible that countries would agree to ratify the change.

Chapter XVIII of the U.N. Charter allows for amendments to the Charter when two-thirds of the members present at a General Conference, including all five permanent members of the Security Council, agree to the change and ratify that change via their respective constitutional processes.[109] While definitely challenging to achieve, the Charter has been amended multiple times throughout its history.[110] In order to create a private sanction for corporate officers, an amendment is needed that would expand the authority of Chapter VI, Article 34 to allow for the investigation of private, non-state actors.[111] The Provisional Rules of Procedure of the Security Council do not provide a mechanism for private parties to appear before the Council in regards to issues that only effect themselves.[112] Adding language that notes that the Security

[108] *See* W. Michael Reisman, *Amending the UN Charter: The Art of the Feasible*, 88 AM. SOC'Y INT'L L. PROC. 108, 108 (1994).

[109] U.N. Charter art. 108.

[110] *See Can the UN Charter Be Amended, and How Many Times Has This Occurred?* UNITED NATIONS DAG HAMMARSKJÖLD LIBRARY (Apr. 27, 2018), http://ask.un.org/faq/140440 [https://perma.cc/Y6B2-2LS6]. The Charter has been amended five times, primarily to enlarge different councils. *Id.*

[111] U.N. Charter art. 34 ("The Security Council may investigate any dispute, or any situation which might lead to international friction or give rise to a dispute, in order to determine whether the continuance of the dispute or situation is likely to endanger the maintenance of international peace and security.").

[112] The only existing means for a private party to appear before the Security Council is when the private individual is providing information regarding a matter related to a member state. *See* United Nations Security Council Provisional Rule of Procedure 37, https://www.un.org/security council/content/rop/chapter-6 [https://perma.cc/DV28-URHC] ("Any Member of the United Nations which is not a member of the Security Council may be invited, as the result of a decision of the Security Council, to participate, without vote, in the discussion of any question brought before the Security Council when the Security Council considers that the interests of that Member are specially affected, or when a Member brings a matter to the attention of the Security Council in accordance with Article 35 (1) of the Charter."); *id.* at Rule 39 ("The Security Council may invite members of the

Council's investigatory powers extend not only to state actors but also to private actors engaged in a global enterprise would be a means of increasing the Security Council's jurisdiction. To narrow the scope of such amendment, language clarifying that these private actors are only subject to sanctions for human rights abuses may make the change more palatable to member states. If data privacy violations are to be the test case for expanding sanctionable parties, then limiting language will still be necessary. As proposed, general language extending authority to private actors still leaves room for many human rights violations that go beyond data privacy violations. To remedy this, additional language in the statue or a clarifying comment by the High Commissioner of Human Rights' office should be added to clarify that this provision should only be invoked for data privacy violations.

3. Avoiding a Veto

The last obstacle to overcome in creating a private sanction is the potential of a veto from one of the five permanent members of the Security Council. Many of the major data-driven corporations are housed in two of the permanent Security Council members' home countries—China and the United States[113]—and member states would likely resist sanctioning their domestic corporate officers. This veto potential is problematic because, even if these countries were to simply refuse enforcing the sanction in their own country, the veto prevents the sanction from coming into effect meaning that other U.N. member states would have no

Secretariat or other persons, whom it considers competent for the purpose, to supply it with information or to give other assistance in examining matters within its competence.").

[113] *See* Sally French, *China Has 9 of the World's 20 Biggest Tech Companies*, MARKETWATCH (May 31, 2018), https://www.marketwatch.com/story/china-has-9-of-the-worlds-20-biggest-tech-companies-2018-05-31 [https://perma.cc/C5QE-VK74]. China and the U.S. dominate the tech market, splitting all top twenty slots between themselves. *Id.*

sanction to enforce at all.[114] A veto would force member states to rely on their own domestic systems to create sanctions, which may be less likely to have the desired effect of a global, uniform sanction regime. Additionally, the five permanent members negotiated their veto power as a condition of their joining the UN,[115] and eliminating it may trigger some of the most important superpowers to withdraw their membership, which would imperil the viability of the U.N.

In order to make sure that a sanction is possible without being subjected to a potentially biased veto, it may be necessary to amend the U.N. Charter to eliminate the veto power of the permanent Security Council members. Article 27(3) of the U.N. Charter requires the "concurring votes of the permanent members,"[116] which means that if any permanent member votes against a resolution, it fails. Using the amendment procedures discussed above in relation to expanding authority of the council to target private individuals, the General Assembly could meet and vote to eliminate the language requiring permanent members' concurrence. However, the likelihood of a measure eliminating the veto power passing is incredibly low with the dual requirements of a two-thirds vote by member states and affirmative votes from all five of the permanent Security Council members.[117]

Making changes to the Security Council's veto power has been a recurring suggestion for years.[118] One of the most

[114] *See The Veto*, SECURITY COUNCIL REP., (Feb. 8, 2019), https://www.securitycouncilreport.org/un-security-council-working-methods/the-veto.php [https://perma.cc/8SV4-YYPJ].

[115] Gareth Evans, *Should the UN Security Council Veto Be Limited?*, WORLD ECON. F. (Feb. 5, 2015), https://www.weforum.org/agenda/2015/02/should-the-un-security-council-veto-be-limited/ [https://perma.cc/GA3P-RV4W] ("The right to veto was the price demanded by China, France, Great Britain, Russia, and the US for joining the UN. No one believes that a formal Charter amendment to abolish or limit this right is remotely likely.").

[116] U.N. Charter art. 27, ¶ 3.

[117] *See* Evans, *supra* note 115.

[118] *See* N.Y. UNIV. CTR. ON INT'L COOPERATION, PATHWAYS TO SECURITY COUNCIL REFORM 4 (2014), https://cic.nyu.edu/sites/default/files/pathways_sc_reform_final.pdf [https://perma.cc/6MQX-Q5RR].

recent proposals for change requested that permanent members refrain from using their veto powers according to the "responsibility to protect" ("R2P") principle in cases of mass-atrocities.[119] Reframing of the R2P principle—which does not eliminate the veto power completely—could allow an expansion of the veto refrain to include cases of widespread data privacy violations. While not remotely close to genocide or mass killings, data privacy violations, as discussed above, do constitute human rights violations and often occur on a large scale that can affect billions of people globally.[120] In such limited cases, which would ideally be the target of corporate officer sanctions, it would be reasonable to ask the permanent members of the Security Council to refrain from using their vetoes.

Another possible mechanism for overcoming the veto would be to alter the U.N. Charter and allow the U.N. General Assembly to override a Security Council veto. The problem of getting consensus from all five permanent Security Council members still remains a problem, however.

Yet, there may be a method for overcoming vetoes that already exists in the U.N. framework. Overriding vetoes is not without precedent; Resolution 377A—"Uniting for Peace"—was passed by the U.N. in 1950 to allow assistance to South Korea after Russia attempted to veto an intervention.[121] Resolution 377 allows for U.N. action, without Security Council consensus, when international peace and security are

[119] *Id.* at 10. Additionally, permanent members have obligations under the U.N. Charter, as well as international humanitarian and human rights law, not to undermine the effectiveness of the U.N. or that body of law. *See* CITIZENS FOR GLOB. SOLS., THE RESPONSIBILITY NOT TO VETO: A WAY FORWARD 6 (2010), http://responsibilitytoprotect.org/Responsibility_not_to_Veto_White_Paper_Final_7_14__2_.pdf [https://perma.cc/CA59-TMMG].

[120] *See* Amerding, *supra* note 2.

[121] Peter Tatchell, *There Is a Way to Override Russia's UN Veto – and Save Aleppo Before It's Too Late*, TELEGRAPH (Oct. 27, 2016), https://www.telegraph.co.uk/news/2016/10/27/there-is-a-way-to-override-russias-un-veto--and-save-aleppo-befo/ [https://perma.cc/ZY82-7T2T].

endangered.[122] This is the most promising mechanism for avoiding a veto in cases when corporate officers perpetuate data privacy violations, because such violations would have global impact or severe enough effects to raise international alarm. Thus, these events would likely carry enough salience to garner enough votes to overcome a veto at either level.

Other common proposed tactics for changing the power of the Security Council would involve expanding the Council to include other new permanent members or expanding seats on the Security Council generally.[123] However, increasing permanent membership would only exacerbate the problem of state protectionism, and increasing general membership would not diminish the possibility of a veto. Thus, these tactics would be of little use to this Note's proposed strategy for targeting corporate officers and avoiding a veto by a member state. The ultimate goal of creating a sanction that can reach corporate officers directly for their roles in data privacy violations, suppression of evidence of misappropriation, and other data misappropriations will likely require a total reworking of the U.N. sanctioning regime. While the prospect of amending the U.N.'s functionality in this way is admittedly lofty, member states would ultimately benefit from the protection that this system would afford. Data protection and accountability are critical to the protection of private interests, governmental affairs, and the economies of all member states. Given the U.N.'s ability to reach into and affect almost every country, it would be logical for the international entity to establish oversight over private individuals in the data privacy space.

---

[122] G.A. Res. 377 (V) A, Uniting for Peace (Nov. 3, 1950) ("Upon the invitation or with the consent of the State into whose territory the Commission would go, the General Assembly, or the Interim Committee when the Assembly is not in session, may utilize the Commission if the Security Council is not exercising the functions assigned to it by the Charter with respect to the matter in question. Decisions to utilize the Commission shall be made on the affirmative vote of two-thirds of the members present and voting. The Security Council may also utilize the Commission in accordance with its authority under the Charter[.]").

[123] *See* Call for Removing Veto Power, *supra* note 100.

V. CONCLUSION

The expanding nature of data processing and where that data is processed has opened users up to a whole range of possible privacy exposure points.[124] The globalization of data-driven companies means that users' personal information can be acquired, stored, or transferred through any number of countries and exposed to the risk of misappropriation.[125] The lack of clarity in user agreements, or in some cases, the lack of any agreement at all, means that users do not necessarily know how or by whom their data is being used.[126] Corporate officers have an obligation, as the heads of their respective companies, to treat what is often individuals' most sensitive information with heightened care. Unfortunately, officers have not taken that care consistently, and a number of companies have exposed their users to the highest levels of both cyber and physical harm.[127] The repeated hacking of data centers and the sharing of data with untrustworthy sources has left users frantic because these companies often offer services that feel compulsory to use, and because it is almost impossible to separate oneself from them without suffering some kind of adverse blowback.

While the possibility of allowing the U.N. to sanction corporate agents for their allowance or perpetuation of gross data privacy violations is ambitious, it certainly is not unreasonable. This Note proposes that creating the pathway to sanction these private actors with asset freezes, travel restrictions, and bans on their technology being used across

124 *See* Juliana De Groot, *The History of Data Breaches*, DIGITAL GUARDIAN (Jan. 3, 2019), https://digitalguardian.com/blog/history-data-breaches [https://perma.cc/T36R-QSKV].

125 *See* Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, INFO. TECH. & INNOVATION FOUND. (May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost [https://perma.cc/AQ64-P63R].

126 *See* Alex Hern, *Privacy Policies of Tech Giants 'Still Not GDPR-Compliant'*, GUARDIAN (July 4, 2018), https://www.theguardian.com/technology/2018/jul/05/privacy-policies-facebook-amazon-google-not-gdpr-compliant [https://perma.cc/7T2A-4N6F].

127 *See* Amerding, *supra* note 2.

borders would create an effective deterrent that would hopefully propel more corporate agents to uphold international standards of data privacy and to protect those whose data they use for the benefit of their companies. Such an aggressive approach would hopefully allow for more global accountability and force companies to respect data privacy in all countries, not just those that strongly regulate data privacy.