# AN INTERNATIONAL APPROACH TO DATA PRIVACY

## POLICY BRIEFING NOTE

AUGUST 2018

CMSI
CENTER FOR MEDIA & SOCIAL IMPACT
SCHOOL of COMMUNICATION
AMERICAN UNIVERSITY • WASHINGTON, DC

DR. ARAM SINNREICH

# ABOUT THE PROJECT

## Policy Briefing Note: An International Approach to Data Privacy

This policy briefing is part of an ongoing research agenda conducted across several schools and research centers within American University, geared toward understanding the increasingly central role of data in our public and civic lives. A related event on data privacy in the United States, co-hosted by the School of Communication, the Internet Governance Lab, and the Internet Society (ISOC), will take place in Autumn, 2018.

## About the Center for Media & Social Impact

The Center for Media & Social Impact (CMSI) at American University's School of Communication, based in Washington, D.C., is a research center and innovation lab that creates, studies and showcases media for social impact. Focusing on independent, documentary, entertainment and public media, CMSI bridges boundaries between scholars, producers and communication practitioners who work across media production, media impact, public policy and audience engagement. The Center produces resources for the field and research, convenes conferences and events and works collaboratively to understand and design media that matter. www.cmsimpact.org.

CMSI
CENTER FOR MEDIA & SOCIAL IMPACT
SCHOOL of COMMUNICATION
AMERICAN UNIVERSITY • WASHINGTON, DC

# ABOUT THE AUTHOR

## Dr. Aram Sinnreich

Dr. Aram Sinnreich is an Associate Professor and chair of the Communication Studies division at American University's School of Communication. Sinnreich's work focuses on the intersection of culture, law and technology, with an emphasis on subjects such as emerging media and music. He is the author of three books: *Mashed Up* (2010), *The Piracy Crusade* (2013), and *The Essential Guide to Intellectual Property* (2019). He has also written for publications including *The New York Times, Billboard, Wired, The Daily Beast*, and *The Conversation*. Previously, Sinnreich served as Associate Professor at Rutgers University's School of Communication and Information, Director at media innovation lab OMD Ignition Factory, Managing Partner of media/tech consultancy Radar Research, Visiting Professor at NYU Steinhardt, and Senior Analyst at Jupiter Research. He is also a bassist and composer, and has played with groups and artists including progressive soul collective Brave New Girl, dub-and-bass band Dubistry, and Ari-Up, lead singer of the Slits. Along with co-authors Dunia Best and Todd Nocera, Sinnreich was a finalist in the 2014 John Lennon Songwriting Contest, in the jazz category.

# TABLE OF CONTENTS

# Summary

With the enforcement of the European General Data Protection Regulation (GDPR) in effect as of May, 2018 and the ongoing furor regarding the role of Facebook user data in "microtargeting" disinformation campaigns by political consultancy Cambridge Analytica during the 2016 U.S. presidential and Brexit campaigns, the subject of data privacy has garnered increasing visibility and concern in recent years. Yet, while this renewed focus has contributed directly to some state, national, and regional policies aimed at stemming the collection and misuse of consumer data, the threats of data insecurity continue to outpace the efforts to contain it. This policy brief argues that an international approach to standardizing and coordinating proactive data protection policy, ultimately mediated via existing treaty organizations, will play an important role in turning the tide and restoring data security and privacy on a global scale.

## Data Insecurity is a Threat to Markets and Governments

It is difficult to overstate the risks posed by data insecurity, both today and in the foreseeable future. While business analysts have argued for decades that consumer data would become the primary resource exploited by internet-based industries, the past five years have seen a massive explosion in the scope and sophistication of data harvesting and analysis technologies. This infrastructure has been developed in large part due to economic incentives in the digital marketing sector, with consumer-facing companies like Google, Amazon, and Facebook leading the way, but with significant assistance from "back-end" data harvesting and analysis companies like eXelate (acquired by Nielsen in 2015) and Acxiom. Additional development has emerged from the defense contracting arena; according to a recent report by business intelligence firm Govini, U.S. government expenditures on big data, artificial intelligence (AI) and the cloud climbed 32% over the past five years, to $7.4 billion in 2017. Market research firm IDC anticipates spending on big data and analytics will continue climb even more steeply, from about $8 billion in 2016 to $13.3 billion in 2021.

Yet, while the data harvesting infrastructure has been built to augment commercial profit and national security, the effects of these technologies pose serious threats to both set of interests. Already, high-profile data breaches at companies like Yahoo, Target, Equifax, eBay, and Adult Friend Finder have compromised data from billions of accounts, leading to major financial losses in each case. The Yahoo hack, for instance, diminished the company's sale price by an estimated $350 million. Even more recently, Facebook lost roughly $120 billion in market value in a single day, due to declines in both revenue and user growth, linked in part to concerns over the Cambridge Analytica (CA) scandal and internal efforts to compensate for it. Consumers have borne the brunt of these hacks, as well — not only indirectly via their relationships with these companies, but due to the criminal exploitation of the data harvested by hackers.

The threats of data insecurity to governments and democratic processes is equally well documented, and even more concerning. Cambridge Analytica used Facebook user data, without permission, to fuel its microtargeting and disinformation campaigns in nations including the US, UK, Mexico, India, Kenya, the Czech Republic, Argentina, and Nigeria. These data, when combined with those extracted from government databases such as voter rolls, become even more potent weapons against free and fair elections. Though CA has shuttered in the wake of its scandals, and governments have become more alert to the potential threats of data hacks, both elements of this toxic combination are still in play. Several principals of Cambridge Analytica co-founded a successor firm, Emerdata, in August, 2017, and its methodology has been emulated by countless additional political consultancies and even less savory interests. Government data breaches have continued unabated, as well. In the US, at the time of writing, reporters have already documented active measures by Russian military intelligence to hack Senate campaigns, voting systems, and private election companies in advance of the 2018 midterm elections. Additionally, national data systems fom the Office of Personnel Management to the electrical grid have been breached, exposing data on citizens, federal employees and crucial infrastructure to hackers.

Ultimately, these breaches of data security have unquantifiable consequences that extend beyond any specific company, election, or nation. The loss of data privacy undermines investor and consumer confidence in the marketplace, voter confidence in democratic governance, and citizen confidence in the legitimacy of government and the sanctity of human rights, threatening the very foundations of liberal democracy around the world.

## Current State of Data Privacy Regulation

Governments have voiced concern about data privacy since the initial growth of the consumer internet in the mid-1990s. Yet, despite the existence of poorly-conceived anti-hacking laws like America's Computer Fraud and Abuse Act (CFAA, 1986) and rudimentary ones like the European Privacy Directive (1995) and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA, 2000), there was little in the way of comprehensive data privacy regulation prior to the 2013 revelations of mass government surveillance by NSA contractor Edward Snowden.

Over the past five years, as the volume of consumer data captured and exploited by states, commercial entities and criminal interests has grown precipitously, there has been a commensurate rise in legislation and policy aiming to limit the use of such data. Perhaps the most sweeping and high-profile example is the General Data Protection Regulation (GDPR), a European Union regulation adopted in 2016 that went into effect as of May, 2018. The regulation requires informed, revocable consent from consumers before their data is collected, processed, or exploited — as long as either the consumer or corporation in question is located within the EU. Because of the EU's size and political and economic centrality, this regulation has had considerable effects beyond its borders, as companies based in the United States, China, and elsewhere around the globe reconfigured their own technologies and policies in order to continue doing business with EU citizens.

Other states have proposed or enacted data privacy regulations, as well. In anticipation of its exit from the EU, the UK passed the Data Protection Act of 2018, which implements the GDPR under national law. Brazil, which passed legislation protecting a broad suite of "digital rights" in its Marco Civil da Internet in 2014 (reportedly, the bill gained steam following Snowden's revelations about American surveillance of Brazilian internet traffic), is now in the process of legislating its own version of GDPR, and the creation of a government body called the National Data Protection Authority. In the U.S., California also recently passed its own data privacy law, which gives consumers in that state the ability to audit all of the commercial data that has been collected about them, access to a full list of third parties with permission to use their data, and a legal mechanism to sue companies that violate its terms. Additionally, bilateral agreements like the EU-US Privacy Shield aim to create facilitate and regulate the flow of consumer data between commercial entities on either side of the Atlantic.

Despite these recent gains on the data privacy front, there are still significant challenges to stemming the tide of data abuse on a global scale. Thus far, for instance, the United States has failed to develop federal laws or regulations akin to the GDPR. Some legal scholars have opined that the First Amendment, broadly interpreted, prevents the government from exerting prior restraint on corporate use of data (this premise has yet to be tested in the case of California). In Canada, the forward-thinking PIPEDA has not been updated to reflect the level of privacy ensured by the GDPR; despite a 2015 amendment that included mandatory notification of data breaches, an amendment providing stronger enforcement powers, C-475, was defeated in 2014.

Finally, even for those laws and regulations that have been enacted successfully, there are ample criticisms of their social effects from every side. Free speech and free market advocates alike decry that the policies are overbroad in their scope, placing unnecessary obstacles in the way of the flow of public information and imposing unnecessary costs for compliance on well-intentioned commercial entities, undermining the ability of corporations to compete on an even playing field. On the other side, privacy advocates argue that the policies don't go far enough, creating what advocate Max Schrems has called a "take it or leave it" environment in which consumers are coerced into ceding their personal data in exchange for access to vital services.

## Outlook: Data Privacy Concerns Will Intensify

The technological and social conditions that have precipitated the current crisis will intensify sharply in the years to come, if current trends continue, making it increasingly vital that every internet user enjoys legally enforced data privacy protections.

One contributing factor will be the rapid development and adoption of networked sensor devices, both in the consumer marketplace and in the public infrastructure. These devices, which are typically grouped under the rubric of the Internet of Things (IoT), are becoming more powerful, less expensive, and more widely proliferated with every passing year. Though market estimates vary widely, they all predict a sharp upward trend and a high volume of spending; for instance, Bain predicts that business-to-business (B2B) IoT sales will top $300 billion by 2020, and Boston Consulting Group projects a figure of $267 billion. Along similar lines, most market research firms estimate that there are between 20-30 billion IoT devices currently online and that the number may triple over the next five years.

What does it mean economically and politically that there are already three internet-connected sensor devices for every person on the planet, and that the number is likely to grow precipitously in the near future? In short, the answer is that both factors in the toxic combination that contributed to the political disruptions of 2016-18 will be significantly amplified. "Surveillance capitalism" companies, such as Amazon, Facebook, Google and Apple, will extract a broader array of data on a more frequent basis than they have in the past, using devices such as in-home "smart speakers," wearable computing devices such as "smartwatches," and automotive "smart car" accessories backed by increasingly sophisticated AI such as Siri and Alexa. At the same time, public and industrial spaces will be increasingly outfitted with not only networked video monitoring devices, but a broad array of sensors that will make it increasingly easy for law enforcement and employers to identify and collect data on individual citizens. Government surveillance data, already at significant risk of third-party intrusion, will not only grow in scope, but will increasingly be analyzed and stored in the form of actionable intelligence, such as the "social credit system" China plans to implement in the coming years. Finally, new quantum computing capabilities are likely to render most forms of standard encryption obsolete in the near future, meaning that even private data and communications transacted over the internet will be rendered legible to any third party with the financial wherewithal to afford the processing power.

Without adequate legal and technological protection, internet users and private citizens around the world will face ongoing and escalating privacy risks that will make them increasingly vulnerable to criminal exploitation, institutional intimidation, and political manipulation. Ultimately, with the pace of change only accelerating, any reactive or voluntary policies aimed at shoring up data privacy will inevitably fall short of the mark. The only workable solution to protecting markets and governments over the

long term is a proactive, global-scale approach to data policy.

## Proposal: Internationalize Data Privacy — First Locally, Then Via Treaty Organizations

There is no "silver bullet" for our mounting data security challenges and the threats they pose to liberal democracies. However, there are both shorter and longer term strategies that may help to mitigate the crisis. In the shorter term, every nation with a stake in internet governance and a role in promoting democratic values should focus on creating its own data privacy laws. As mentioned above, the enactment of the GDPR immediately required companies spanning the globe to update their privacy policies, because the risk of non-compliance represents the potential loss of European customers (and their legally-obtained data). If Brazil successfully follows suit, it will further normalize GDPR-level data protections internationally.

Canada is a prime candidate to be another early mover in this arena. As departing Internet Society CEO Kathy Brown remarked earlier this year, Canada is already "taking the lead to convene necessary stakeholders to address privacy and security challenges around the exploding Internet of Things."[1] The country should parlay this leadership role into a broader mandate to take the reins when it comes to privacy in the North American context, and pass a bill emulating or even improving on GDPR.

Due to a variety of factors including its polarized political climate, the United States is less likely to lead the charge on data privacy protections. However, if more populous states like California continue to pass their own data privacy laws and defend them successfully against challenges in the courts, there may be enough momentum to translate these policies to the federal level. The idea already has support with the American legislature; Senator Mark Warner, for instance, has proposed that the U.S. "adopt rules mirroring GDPR."[2] Senators Amy Klobuchar and John Kennedy co-sponsored a recent bill called the Social Media Privacy Protection and Consumer Rights Act, and Senators Richard Bulenthal and Ed Markey proposed another one called the CONSENT Act. If both these bills were passed into law, they would collectively provide much of the data privacy protection currently afforded to EU residents.

Over the longer term, however, because of the global interdependencies inherent to the internet and the data flows it enables, multilateralism will be the most effective route to securing consumer data and preserving functional democracies and markets. Towards this end, nations that support strong consumer data privacy regulation should work with existing treaty organizations to enforce a universal standard. Specifically, a treaty administered by the World Trade Organization (WTO) would require member states to implement laws that affirm fundamental data privacy rights, specify regulatory thresholds, and establish institutional bases for policing and prosecuting violators.

While many treaty organizations may serve as appropriate administrators for a global data privacy accord, the WTO makes the most sense both because of its fundamental focus on lowering international trade barriers and because of its unique all-in organizational structure. There are drawbacks to this plan, of course. The organization itself currently acknowledges it "has had had nothing whatever to do with Internet privacy"[3] and has historically come under criticism for undermining sovereign privacy protections. Politically, the present moment is not optimal for WTO leadership on the issue; between the new antipathy toward trade exhibited by the current U.S. administration and the ascendancy of countries with weaker records on human rights like Russia and China, the organization may seem unsuited to the task of regulating commercial data. Yet it is still the most influential and central site for international trade accords, and it already has the apparatus in place not only to administer data privacy protections but, most importantly, to make economic relations contingent on their faithful execution.

Founded in 1995, the WTO represented a new era in international trade. Not only did the organization supersede existing bilateral and multilateral trade agreements, it grouped previously disconnected trade-related issues including commodities, services, intellectual property, and financial services under one umbrella. Rather than picking and choosing the nature of their reciprocal economic relationships, member states (there are currently 164) must adhere to all aspects of membership; thus, if member nation X wants to trade a given commodity with member nation Y, it must also abide by shared intellectual property and financial regulations under the agreement.

By adding a new data privacy accord to the roughly 60 different agreements currently overseen by the WTO, member nations could with a single swipe of the pen create global conditions of regulated data privacy, covering the vast majority of consumers and citizens around the globe, in addition to nearly every company that collects, analyzes and deploys consumer data in the course of its operations. Like other WTO-administered agreements, this data privacy accord would recommend minimum thresholds for data privacy laws within member nations (for

instance, mandating a maximum duration of data retention, required text for privacy policies, or minimum penalties for negligent data breaches), and it would serve as an international site for the resolution of disputes related to data privacy on our international communication networks. Additionally, it would leave very few places on the planet safe for abuse of consumer data; as with other violations of WTO-administered accords, the penalty for non-compliance would be potential tariffs and even ejection from the organization, creating strong economic disincentives for nations to fail in their pledge to police data abusers.

A WTO-administered data privacy agreement would necessarily be part of a broader coordinated effort to curb the exploitation of consumer data, in partnership with telecommunications and technology companies, as well as international law enforcement bodies. Even in the best case scenario, it wouldn't prevent *all* cases of data abuse, just as its IPR agreements don't curb all international piracy. But it would lay the political foundations for a sea change in global awareness and governance of consumer data, and in so doing, might provide the necessary framework for the preservation of liberal democracy and free markets.

# APPENDIX

# END NOTES

[1] https://www.internetsociety.org/news/speeches/2018/kathy-browns-remarks-internet-jurisdiction-conferences-opening-session/
[2] https://www.scribd.com/document/385137394/MRW-Social-Media-Regulation-Proposals-Developed
[3] https://www.wto.org/english/tratop_e/serv_e/gats_factfiction10_e.htm

# AN INTERNATIONAL APPROACH TO DATA PRIVACY

## POLICY BRIEFING NOTE

CMSI
CENTER FOR MEDIA & SOCIAL IMPACT
SCHOOL of COMMUNICATION
AMERICAN UNIVERSITY • WASHINGTON, DC

www.cmsimpact.org

©2018. All Rights Reserved.