THE NATIONAL SECURITY INSTITUTE
At George Mason University's Antonin Scalia Law School

COMBATING DIGITAL AUTHORITARIANISM:

U.S. Alternative Needed to Counter Data Localization and Government Control

By DR. ANDREA LITTLE LIMBAGO

Senior Fellow and NSI Associate Director of Emerging Technologies

THIS REPORT:

1

Describes the global trend toward data localization—policies that require data to be stored within national borders and often impede cross-border flows.

2

Explains the digital divide between authoritarian regimes' use of data localization as a key means of information and political control, and more nascent efforts at a democratic alternative.

3

Argues that a U.S. data privacy and security framework is needed to counter the rising authoritarian model that is fostering a global splinternet and debilitating democratic values across the globe.

Dr. Andrea Little Limbago is the Chief Social Scientist at Virtru, where she specializes in the intersection of technology, national security, and society. She is also the Associate Director for the Emerging Technologies Program at the National Security Institute at George Mason, and has previously held leadership positions in the Department of Defense and taught in academia.

I INTRODUCTION AND EXECUTIVE SUMMARY

Global data laws are reshaping the internet with profound implications for U.S. national security and economic prosperity. From the European Union's General Data Protection Regulation (GDPR) effort to protect citizens' data to Russian and Chinese laws mandating access to encryption keys, source code, or other sensitive data, foreign data laws are shaping global privacy, security, and innovation.

The United States currently pursues industry-specific or state-centric data laws and has yet to formulate a comprehensive framework to guide democracies in the pursuit of both data protection and innovation. This paper explores current global trends in data regulation and localization that may fragment the Internet and reshape norms in critical areas, eroding trust in cyberspace. The paper also offers observations about what the U.S. can champion on the world stage to remain relevant and resist Balkanization.

Global surveillance, censorship, and digital attacks remain defining features of the global security landscape. To gain greater control of information within their borders, states are increasingly pursuing data regulation and localization laws that reflect their values and priorities. Many authoritarian regimes are pursuing forced localization, requiring data to be stored within their borders and impeding cross-border flows.

Conversely, the GDPR and subsequent democratic models allow the relative free flow of data while focusing on individual rights and control.

The current U.S. patchwork approach is ill-equipped to win the growing international competition to set standards for the use and control of data. The United States should work with the private sector to formulate a comprehensive, federal framework for data privacy and security. Absent a more holistic approach, foreign laws will continue to shape the global digital economy for the foreseeable future, stifling economic innovation or at worst undercutting democracy, civil liberties, and U.S. national security.

CORE COMPONENTS OF A U.S. DATA PRIVACY & SECURITY FRAMEWORK SHOULD INCLUDE:

- **CONTROL:** Individuals and organizations become empowered to customize data access and protections
- **TRANSPARENCY:** Clarity and broader comprehension across all aspects of data protection and sharing, including terms of service and third-party access
- **ACCOUNTABILITY:** Legal consequences for organizations that fail to take meaningful steps toward data protection or infringe on data protection
- **INTEROPERABILITY:** Common standards that promote both data protection and cross-border data flows regardless of industry

II BACKGROUND ON THE DATA DIVIDE

Over two decades ago, Alphabet CEO Eric Schmidt noted, *"The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had."*

This ongoing experiment in anarchy is at an inflection point, as governments attempt to instill various controls over the internet within their borders. In some cases, governments pursue individual security and privacy, but increasingly governments across the globe enact domestic data protection policies wherein the government is the main arbiter and moderator of data. While it is a common refrain that policy, law, and ethics lag behind technology, this is not necessarily the case for authoritarian regimes.[1]

While democracies have generally grasped onto utopian visions of the Internet as a key promoter of democracy, information diffusion, and economic development, authoritarian states have quickly embraced digital changes and innovations to further entrench regime durability, including information control and manipulation. They often promote new models of Internet governance that focus on cyber sovereignty, or governmental control of digital data and the Internet within sovereign borders.

Data localization policies and laws are a key mechanism for achieving cyber sovereignty—requiring data or domains to physically operate or be accessible to governments within national borders. This greatly impacts cross-border data flows and international business while giving authoritarian regimes unique access to personally identifiable and commercial data—expanding the capacity for political and social control.[2]

III DATA LOCALIZATION KEY TO THE AUTHORITARIANS' GLOBAL DIGITAL STRATEGY

For decades, authoritarian and quasi-democratic regimes have pursued strategies exploiting Internet expansion for information control. Domestic strategies in turn become the testbed for international digital activity, and also may be replicated by other states.

China's Great Firewall has sparked similar aspirations in Iran's Halal Network and in Russia as well—instigating discussions of a global "splinternet" as opposed to a globally integrated system. Global powers are in a battle over the role of government in the global digital future, and it sometimes appears the authoritarian regimes are winning by achieving "first mover" advantage.

Data localization is a core component of strategies based on information control. By requiring domestic data storage and unrestricted and data access, governments can maintain greater control over individuals and information within their borders. It also facilitates the ability to limit what data exists within a country and block social forums that don't allow the access demanded. Increasingly, many of the new data localization components (e.g., new laws in Vietnam[3] and Thailand[4]) fall under broader cybersecurity legislation

that also involves elements of censorship, especially with regard to controlling anti-government rhetoric.

For instance, in 2005 **Kazakhstan** required all .kz top-level domain names to operate on servers within its borders.[5] In **Iran**, extensive online censorship coupled with requirements for local data storage from apps such as WhatsApp and Telegram are key components of their information control. Importantly, these tactics have expanded into weak democracies such as **Turkey** where the Law on the Protection of Personal Data limits the transfer of personal data out of Turkey, while requiring some data stored in country as well. In fact, a similar law a decade earlier targeting Internet-based payment services led PayPal to withdraw.

As the core proponents of an information control strategy are relying on data localization, it's important to comprehend the Chinese and Russian strategies, because they are quickly inspiring others across the globe.

China has adopted an aggressive and acquisitive approach to digital life, controlling access to information and accumulating vast amounts of data on its citizens and those of other countries.

In short, China's approach to information control is multi-pronged, including astroturfing as a form of censorship, data access requirements, and 'security checks' on data flows across borders.

CHINA'S GREAT FIREWALL

The "Great Firewall"—a term first dubbed in 1997—is the most prominent example of a country's attempt to control information and data flows within its borders.[6] The Great Firewall aims to censor and control information within China's borders through a combination of legislative policies as well as technical solutions, such as URL filtering that denies access to certain sites and blocking Virtual Private Networks (VPN). Over the years, China has extended this approach, not only blocking what information goes into and out of China, but also what is discussed within the borders.

THE CYBERSECURITY LAW

The Cybersecurity Law of the People's Republic of China came into force in June 2017, and extends data localization into "critical information infrastructure", requiring access to foreign companies' data, as well as local storage of data.[7] For over a decade, China has demanded foreign corporations turn over data, but this new law tightens the requirements and blacklists corporations who fail to comply.[8] Apple, for example, now stores Chinese user data in southern Guizhou province, including cryptographic keys to unlock the accounts.[9] These policies also sync with China's push toward indigenous innovation and Made in China 2025, including the government control of foreign intellectual property and access to personally identifiable information.[10]

50 CENT PROPAGANDA

China additionally pursues information control and strategic objectives through astroturfing. Domestically, China's 50 Cent Army helps promote pro-government rhetoric, flooding online forums to drown out negative comments. Yet China also seeks to portray itself as a defender of openness, security, and cooperation, as depicted in China's International Strategy for Cyberspace from 2017.[11] Upon the release of the strategy, a government news agency noted that China will help train developing countries and establish global norms as reflected in the strategy.[12]

COMMERCE BY THEFT

The U.S.-Sino pact against cyber-enabled theft for commercial purposes fits into this general pattern.[13] According to a recent United States Trade Representative report, China has failed to comply despite rhetoric to the contrary.[14] These efforts are consistent and reinforce the influence sought through China's United Front department, which seeks to extend Chinese influence globally both through information interference and infiltration into foreign political and economic systems.[15]

SOCIAL CONTROL

Finally, as part of China's comprehensive information strategy, China's social credit system consumes vast amounts of commercial and personal data to track and rate the reputations of individuals and businesses, ultimately cutting off underperformers from banking, travel, employment and other aspects of society.[16]

Russia sees the collection and control of data and surveillance as critical government tools, and has a variety of legal regimes that affect policy and the private sector.

Russia's 2016 information security doctrine outlines its far-reaching approach, including an integration of both the technical and the social and psychological components of digital information control[17]—often first deploying these information security tactics domestically before taking them abroad.[18]

FROM LOCALIZATION TO CYBER SOVEREIGNTY

Russia has quickly progressed from localization policies to seeing advantage in a more robust model of cyber sovereignty. Russia's 2015 Personal Data Law mandates that any data on Russian citizens must be located on servers in Russia.[19] Russia's 2016 law extended these restrictions, requiring users' communications to be stored for six months, while mandating that Internet service providers and telecommunications companies deny service to users who refuse to confirm their

identity per law enforcement requests. Russia also requires foreign companies to provide source code for security products as a cost of doing business there.[20] Most recently, Russia announced a plan to disconnect from the global internet[21] and create a Russian Internet space (Runet).[22]

TARGETING ANONYMITY

Two pieces of legislation in 2017[23] further the focus on data control, eliminating anonymity online and restricting tools to evade censorship, including VPNs and anonymizers.[24] Recently, Russia has pressured Facebook to detail how it is adhering to these laws,[25] and is stepping up pressure on foreign corporations for compliance, while LinkedIn was banned for non-compliance.[26]

THE PROPAGANDA OF CONTROL

State-run media plays a key role in the information security strategy, including the push for greater cyber sovereignty and government-controlled data localization. Under the auspices of the benevolence of virtual borders, the Russian government ostensibly serves as the moderator and protector of personal data against illegal access. Following the debacle surrounding the Telegram ban following its refusal to provide encryption keys,[27] one station argued that the end of globalization is here, and "all countries will build virtual borders … it's inevitable, and it's very good for all of us."[28]

Importantly, data localization compliance failures are handled by Roskomnadzor, the state censor and communications watchdog, demonstrating the breadth of Russia's active measures approach to information control through integrating data localization, disinformation, and censorship under a single umbrella.[29]

IV DEMOCRATIC ALTERNATIVES PROMOTE INDIVIDUAL RIGHTS WITHIN A GLOBAL INTERNET

For the most part, democracies have not moved at the same pace as authoritarian regimes in adapting their legislation to match modern technological realities.

Until recently, the democratic West has seen Internet expansion serving as an enabler for expanded liberty and economic opportunity. However, this singular focus on cyber utopia has come at the detriment of understanding and constraining the potential misuse of the Internet as a tool for authoritarian regimes and criminals.

But this is slowly changing, as the impact of the European Union's General Data Protection Regulation (GDPR), which came into effect in May 2018, reaches beyond its borders to establish a democratic, if hotly debated, baseline for individual data security and privacy.

THE EUROPEAN UNION

The General Data Protection Regulation (GDPR) is the most prominent policy that reflects a democratic alternative to the cyber sovereignty model—emphasizing individual privacy and civil liberties over government access and control. While it takes a more prescriptive approach than the United States, it nonetheless reflects democratic norms that are absent from the authoritarian models.

INDIVIDUAL DATA PROTECTIONS

At its core, the GDPR maintains a strong emphasis on individual data protections, which includes personally identifiable information (PII), but extends to content about an individual. Key data protection features within the GDPR include the right to erasure (aka the right to be forgotten), and the right for an individual to access their data and to rectify incorrect data.[30] It is a far-reaching framework that impacts everything from marketing[31] to artificial intelligence[32] to breach notification.[33]

PROMOTING DEMOCRATIC NORMS

The GDPR reflects the political and economic union of 28 democratic members, reinforcing some of the values and norms of individual freedoms, privacy and humans rights that are foundational to the EU.[34] In this way, its data regulation framework intersects with and adheres very closely to its native political institutions—prioritizing the data protection principles and individual rights they believe reinforce democratic institutions.

REGULATORY GLOBALIZATION VS. DATA LOCALIZATION

Importantly, the GDPR introduces data standards that pertain to data of European Union citizens regardless of where the data is held.[35] Even if a corporation is not headquartered in the EU, but they have data on EU citizens, they must comply with the GDPR. Rather than requiring data be maintained and controlled locally then, the EU opted for regulation and supervision over the use of data no matter where it moves.

The EU's push toward individual data protection and privacy is not surprising in the wake of the increasing magnitude and scope of recent data breaches. In turn, with the additional emphasis on corporate responses to data breaches, the GDPR advances specific desired norms for security and privacy within a regulatory framework. While it certainly will continue to evolve over time, and has its critics as a regulatory model, the GDPR sets a precedent for democratic policy innovation to prioritize data protection and privacy as a fundamental right.

WHAT ABOUT THE U.S.?

The United States has historically taken a light-tough regulatory approach, focusing attention on industries with greater perceived risks, and too often maintaining a reactionary stance in managing the digital policy innovations from abroad. And absent a comprehensive national policy framework, various U.S. states are implementing their own data protection legislation.[36]

A SECTOR-SPECIFIC APPROACH

Unlike Russia, China, and the E.U., the United States has largely taken a sector-specific approach to privacy and security, with a general consumer protection backstop in the Federal Trade Commission. While this may have reflected a reasonable risk-based approach to protecting data, widespread data breaches and unintended or non-disclosure of third-party data access has led to increasing demand for an integrated, comprehensive policy toward data protections, security, and privacy. Thus far however, Congress' consideration of broad privacy and data security proposals has produced little tangible results. As one example, the Data Security and Breach Notification Act[37] was introduced a few years ago to consolidate and synchronize disparate state notification laws, but it has yet to advance. Multiple bills were circulated in the 115th Congress.

SELF-POLICING

Many industries, such as healthcare and finance, have established sector-specific approaches to data protection and privacy, and even within those sectors there are distinct protocols that provide additional complexity to the patchwork of regulations.[38] The tech giants offer various degrees of data protection, while maintaining flexibility to innovate by using and sharing data, and making accommodations for certain legal obligations, such as at times sharing with domestic and foreign governments. Public opinion has shifted dramatically over the last year on the use of data, with many favoring stricter regulation of the tech giants.[39]

A GROWING PATCHWORK

Absent a federal government approach to general security and privacy, a patchwork of proposals has emerged among state and local jurisdictions.[40] The city of Los Angeles required Google[41] to store data within the U.S. as a contractual condition, while the California Consumer Privacy Act of 2018 is the first major, cross-cutting legislation focused on user privacy and protections.[42] New York, Tennessee, Missouri and Ohio are among the states that have proposed various degrees of data localization and data flow restriction laws.[43] In Spring 2018, South Dakota[44] and Alabama[45] became the final two states to enact data breach notification laws,[46] each with different notification requirements. Emblematic of the patchwork, each state adopts slightly different definitions of sensitive data. Finally, Georgia's

governor recently vetoed cybersecurity legislation that not only would have hindered defensive security testing, but also would have enabled corporations to retaliate against cyber-attacks by compromising external networks (i.e., hacking back), risking both negative national security externalities and potentially infringements on privacy as well.[47]

COMBATTING DATA LOCALIZATION

Internationally, U.S. policy has been more cohesive. In global forums and trade negotiations, the U.S. has championed an open internet and sought to rally opposition to data localization and other measures of information control. The U.S-negotiated Trans-Pacific Partnership and U.S.-Mexico-Canada Agreement incorporated novel provisions that reflected these principles of free data flows across borders and discouraging requirements to store or process data locally.

V UNIFORM U.S. APPROACH NEEDED

The perceived absence of global U.S. leadership on data protection has created a vacuum, which is quickly being filled by other countries that do not necessarily share the same values of internet freedom and privacy. Neither the U.S. government nor the private sector benefit when other countries dictate global standards and data regulations, especially given that they may not promote democratic values or may hinder corporate innovation.

To remain engaged globally and try to protect its seat at the regulatory policy table, the United States must acknowledge the data localization occurring across the globe and formulate counter strategies that preserve both security and data privacy. The U.S. must lead by example and progress general data standards in line with preserving democratic values and adherence to appropriate data security and privacy principles, while maintaining an environment that continues to foster innovation. Privacy and innovation need not be mutually exclusive.

A uniform federal approach to privacy and security is long overdue, and if enacted could serve to not only promote security and privacy interests in the private and public sectors, but also to provide global leadership and a democratic model to counter the rising authoritarian model that is fostering a global splinternet and debilitating democratic values across the globe.

VI A U.S. FRAMEWORK FOR DATA

There are four key tenets that should guide U.S. data protection and privacy laws: transparency, control, accountability, and interoperability. Each of these must be able to be reasonably adopted without being overly burdensome on smaller businesses. Otherwise, a new framework would risk unintentionally promoting monopolistic industries controlled by incumbent corporations and hinder the competition that drives innovation.

INDIVIDUAL CONTROL AND SECURITY

Individuals, rather than the state, should be the focus for providing greater control of data, with data sharing and data collection that are based on individuals opting into agreements with private sector parties. They should have access to the data, understand how it is used, and easily customize access policies. A variant of the Consumer Privacy Bill of Rights should be revisited, especially for informed consent, to help move toward common definitions for consumer consent.[48] Consumer control must be flexible as the digital economy evolves, and at a minimum should address social media, e-commerce, apps, and web searches. Individual control of data also conceives of rejecting the authoritarian model of unfettered government access to data and source code.

TRANSPARENCY

Robust transparency is critical to realizing individual control of data and an effective democratic alternative. Transparency must be addressed in all aspects of data protections, from the terms and conditions of service to breach notification and third-party access. Clarity is also essential to ensuring the benefits of transparency are realized.

ACCOUNTABILITY

To move security beyond a 'nice to have', there must be accountability, such as when data is compromised or when a vulnerability is discovered. A holistic and enforceable data protection and privacy framework would send a strong signal to the international community that the United States values individual privacy and is serious about data protection. This could be a significant source of soft power offering contrast to authoritarian models that are intent on rejecting individual data privacy in favor of government access and control.

INTERNATIONAL INTEROPERABILITY

Foundational, common standards are essential for ensuring innovation and cross-border data flows are facilitated, not hindered, by new data protection laws. For instance, there are now distinct data breach notification laws in each state plus Washington, DC, Guam, Puerto Rico and Virgin Islands.[49] This patchwork system also applies across sectors, and should be harmonized based along some common standards that can then be customized as needed. Private sector innovation can be fed into international standards work to promote harmonization. Cross-border data flows are essential to a global digital economy, but require baseline common standards to limit the growth of protectionist localization laws.

VII CONCLUSION

With rampant cyber-attacks and surveillance, trust in the Internet is fragile. The movement in some regions toward data localization is further eroding this trust as the authoritarian model continues to spread.

Although the United States has been involved in shaping international standards and norms for cybersecurity, including for the internet of things[50] and the United Nations Group of Governmental Experts focused on implementing cyber norms, the same has not been as true in data protection and privacy law.[51] Absent U.S. leadership, authoritarian data localization and information control strategies will likely continue to facilitate government control of data over the principles of individual security and privacy that are the bedrock of democracies and technological innovation.

The United States should prioritize a national data privacy law and, once enacted, leverage it globally through cooperative forums. Data privacy is not only an economic and civil liberties issue, it is a national security issue. If the United States fails to make progress in these laws, other countries will continue to drive the standards and norms globally, and negatively impact U.S. national security and economic prosperity.

ENDNOTES

1 Vivek Wadhwa, *Laws and Ethics Can't Keep Pace with Technology,* MIT TECH. REV. (Apr. 15, 2014), https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/.

2 Roger Yu, *More U.S. Companies Push Back on Foreign Must-Store-Data-Here Rule*, USA TODAY (Aug. 12, 2017, 9:00 AM), https://www.usatoday.com/story/money/2017/08/12/more-u-s-companies-push-back-foreign-must-store-data-here-rule/558702001/.

3 Euan McKirdy, *'Stalinist' Vietnamese Cybersecurity Law Takes Effect, Worrying Rights Groups and Online Campaigners*, CNN (Jan. 2, 2019, 7:54 AM), https://www.cnn.com/2019/01/02/asia/vietnam-cybersecurity-bill-intl/index.html.

4 *Thailand passes controversial cybersecurity law that could enable government surveillence*, TECHCRUNCH (February, 28, 2018), https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/.

5 Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, ITIF (May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

6 Geremie R. Barme & Sang Ye, *The Great Firewall of China*, WIRED (June 1, 1997, 12:00 PM), https://www.wired.com/1997/06/china-3/.

7 Zolzaya Erdenebileg, *China's New Cybersecurity Law to be Implemented on June 1*, CHINA BRIEFING(Mar. 16, 2017), http://www.china-briefing.com/news/china-new-cybersecurity-law-to-be-implemented-june-1/.

8 Jacqui Cheng, *Congress Unimpressed by Yahoo Apology for China Dissident E-mail Testimony*, ARS TECHNICA(Nov. 6, 2007, 4:30 PM), https://arstechnica.com/tech-policy/2007/11/yahoo-calls-withholding-of-info-on-chinese-arrests-a-misunderstanding/.

9 *Fears for Human Rights as Apple Moves to Store ICloud Keys in China*, SOUTH CHINA MORNING POST (Feb. 24, 2018, 10:45 PM), https://www.scmp.com/news/china/policies-politics/article/2134562/fears-human-rights-apple-moves-store-icloud-keys-china.

10 Lorand Laskai, *Why Does Everyone Hate Made in China 2025?*, COUNCIL ON FOREIGN REL.: NET POLITICS BLOG (Mar. 28, 2018), https://www.cfr.org/blog/why-does-everyone-hate-made-china-2025.

11 *International Strategy of Cooperation on Cyberspace*, XINHUANET (Mar. 1, 2017, 6:01 PM), http://www.xinhuanet.com/english/china/2017-03/01/c_136094371_2.htm.

12 *China Announces Cybersecurity Strategy*, GLOBAL TIMES (Dec. 27, 2016, 8:21 PM), http://www.globaltimes.cn/content/1026015.shtml.

13 Everett Rosenfeld, *US-China Agree to not Conduct Cybertheft of Intellectual Property*, CNBC (Sept. 25, 2015, 1:39 PM), https://www.cnbc.com/2015/09/25/us-china-agree-to-not-conduct-cybertheft-of-intellectual-property-white-house.html.

14 Office of U.S. Trade Representatives, Exec. Office of the President, *Findings of the Investigation Into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974*, (2018), https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

15 Philip Wen, *China Strengthens Global Influence Agency in Government Reshuffle*, REUTERS (Mar. 21, 2018, 7:09 AM), https://www.reuters.com/article/china-parliament-influence/china-strengthens-global-influence-agency-in-government-reshuffle-idINKBN1GX189.

16 Mara Hvistendahl, *Inside China's Vast New Experiment in Social Ranking*, WIRED (Dec. 14, 2017, 6:00 AM), https://www.wired.com/story/age-of-social-credit/.

17 Sean Lawson, *Russia Gets a New Information Security Doctrine*, FORBES (Dec. 9, 2016, 8:00 AM), https://www.forbes.com/sites/seanlawson/2016/12/09/russia-gets-a-new-information-security-doctrine/#52d466cb3fc4.

18 Peter Pomerantsev, *Russia and the Menace of Unreality*, THE ATLANTIC (Sept. 9, 2014), https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/.

19 Jason Verge, *Firms Rethink Russian Data Center Strategy, as Data Sovereignty Law Nears Activation*, DATA CTR. KNOWLEDGE (July 21, 2015), https://www.datacenterknowledge.com/archives/2015/07/21/russian-data-localization-law-spurs-data-center-strategy-changes.

20 Joel Schectman ET AL., *Under Pressure, Western Tech Firms Bow to Russian Demands to Share Cyber Secrets*, REUTERS (June 23, 2017, 5:06 AM), https://www.reuters.com/article/us-usa-russia-tech-insight/under-pressure-western-tech-firms-bow-to-russian-demands-to-share-cyber-secrets-idUSKBN19E0XB.

21 Catalin Cimpanu and Zero Day, *Russia to disconnect from the internet as part of a planned test*, ZDNET, (February 11, 2019), https://www.zdnet.com/article/russia-to-disconnect-from-the-internet-as-part-of-a-planned-test/.

22 Cristina A. Matamoros, *Runet: Russia wants to 'nationalise the internet' but what does that mean?*, EURONEWS (February 13, 2019), https://www.euronews.com/2019/02/12/new-russian-internet-bill-just-another-layer-of-censorship-says-tech-expert.

23 *Russia: New Legislation Attacks Internet Anonymity*, HUM. RTS. WATCH (Aug. 1, 2017, 10:36 AM), https://www.hrw.org/news/2017/08/01/russia-new-legislation-attacks-internet-anonymity.

24 Ksenia Idrisova, *Explainer: What is Russia's New VPN Law All About?*, BBC (Nov. 1, 2017), https://www.bbc.com/news/technology-41829726.

25 Maria Kiselyova, *Russia Asks Facebook How it Complies with Data Law- Ifax*, REUTERS (Apr. 12, 2018, 10:39 AM), https://www.reuters.com/article/us-facebook-russia-data/russia-asks-facebook-how-it-complies-with-data-law-ifax-idUSKBN1HJ2AB.

26 Ingrid Lunden, *Russia Says 'Nyet,' Continues LinkedIn Block After it Refuses to Store Data in Russia*, TECHCRUNCH (Mar. 7, 2017), https://techcrunch.com/2017/03/07/russia-says-nyet-continues-linkedin-block-after-it-refuses-to-store-data-in-russia/.

27 Mariya Petkova, *An 'Internet Civil War' has Erupted in Russia*, ALJAZEERA (Apr. 23, 2018), https://www.aljazeera.com/news/2018/04/internet-civil-war-erupted-russia-180423124936679.html.

28 Julia Davis, *Russia Warms up the Public to the Idea of Virtual Borders*, http://www.juliadavisnews.com/articles-about-russia/russia-warms-up-the-public-to-the-idea-of-virtual-borders/.
29 Garrett M. Graff, *A Guide to Russia's High Tech Tool Box for Subverting US Democracy*, WIRED (Aug. 13, 2017, 7:00 AM), https://www.wired.com/story/a-guide-to-russias-high-tech-tool-box-for-subverting-us-democracy/.
30 GENERAL DATA PROTECTION REGULATION, Art. 17, (2018), https://gdpr-info.eu/.
31 George Lawton, *Accommodating GDPR Email Marketing Regulations a Top Priority*, SEARCHCRM (Dec. 2017), https://searchcrm.techtarget.com/feature/Accommodating-GDPR-email-marketing-regulations-a-top-priority.
32 Sven Jacobs & Christoph Ritzer, *Data Privacy: AI and the GDPR*, NORTON ROSE FULBRIGHT(Nov. 2, 2017), https://www.aitech.law/blog/data-privacy-ai-and-the-gdpr.
33 GENERAL DATA, *supra note* 30, at Art. 33.
34 Mariusz Maciejewski, *Fact Sheets on the European Union: Free Movement of Goods*, EUR. PARLIAMENT (Oct. 2018), http://www.europarl.europa.eu/factsheets/en/sheet/38/free-movement-of-goods.
35 John Tolbert, *The Impact of the GDPR Outside the EU*, IT SECURITY GURU (Jan. 1, 2017), https://www.itsecurityguru.org/2017/01/30/impact-gdpr-outside-eu/.
36 Benjamin Freed, *Without federal action on data privacy, states forge ahead on their own*, STATESCOOP (March 28, 2019), https://statescoop.com/without-federal-action-on-data-privacy-states-forge-ahead-on-their-own/.
37 S.2179 115th Cong. § 1 (2017).
38 Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection
39 Kim Hart, *Exclusive: Public Wants Big Tech Regulated*, AXIOS (Feb. 28, 2018), https://www.axios.com/axios-surveymonkey-public-wants-big-tech-regulated-5f60af4b-4faa-4f45-bc45-018c5d2b360f.html.
40 Amie Stepanovich, *Data Protection in the United States: Where do we go from here?*, ACCESSNOW (Apr. 23, 2018, 1:48 PM), https://www.accessnow.org/data-protection-in-the-united-states-where-do-we-go-from-here
41 Cory, *supra* note 5.
42 CALIFORNIA CONSUMER PROTECTION LAW, https://www.caprivacy.org (last visited Jan. 4, 2019).
43 Cory, *supra* note 5.
44 Sara Goldstein, *South Dakota Becomes 49th State to Enact a Data Breach Notification Law,* DATA PRIVACY MONITOR (Mar. 27, 2018), https://www.dataprivacymonitor.com/data-breach-notification-laws/south-dakota-becomes-49th-state-to-enact-a-data-breach-notification-law/.
45 Andreas T. Kaltsounis & Sara Goldstein, *Last But Not Least: Alabama Enacts a Data Breach Notification Law With Strong Notification and Security Requirements*, DATA PRIVACY MONITOR (May 1, 2018), https://www.dataprivacymonitor.com/data-breach-notification-laws/last-but-not-least-alabama-enacts-a-data-breach-notification-law-with-strong-notification-and-security-requirements/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.
46 *Security Breach Notification Laws*, NAT'L CONF. ST. LEGIS (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
47 Morgan Chalfant, *Georgia Governor Vetoes Controversial Hacking Legislation*, THE HILL (May 8, 2018, 4:05 PM), https://thehill.com/policy/cybersecurity/386770-georgia-governor-vetoes-controversial-hacking-legislation.
48 Press Release, The White House Office of the Press Sec'y, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online (Feb. 23, 2012).
49 Security Breach Notification Laws, *supra* note 46.
50 COMPUTER SECURITY RESOURCE CENTER, https://csrc.nist.gov/News/2018/Report-International-IoT-Cybersecurity-Standards (last visited Jan. 4, 2019).
51 Elaine Korzak, *UN GGE on Cybersecurity: the End of an Era?*, THE DIPLOMAT (July 31, 2017), https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.