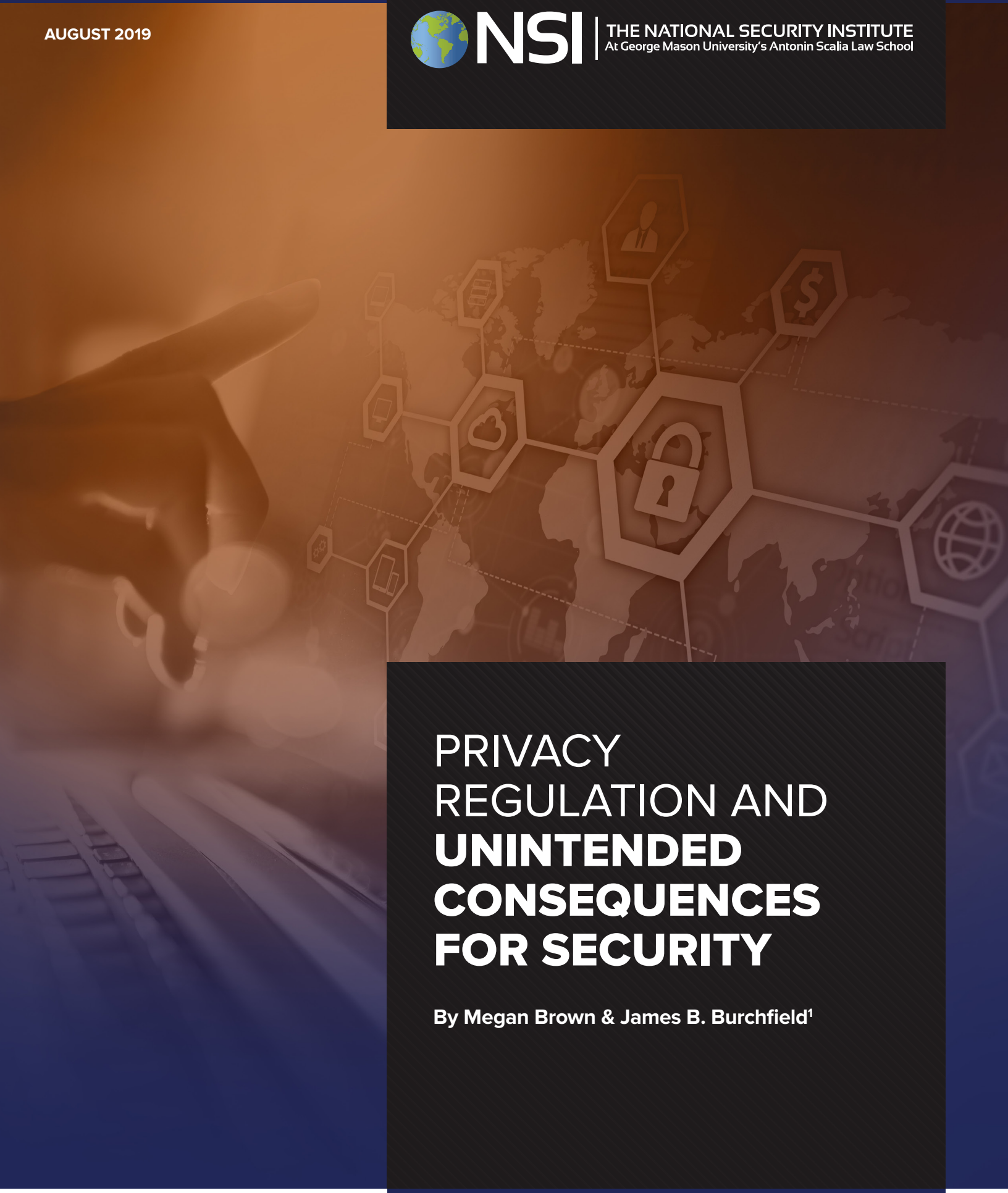
AUGUST 2019

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



PRIVACY REGULATION AND **UNINTENDED CONSEQUENCES FOR SECURITY**

By Megan Brown & James B. Burchfield[1]

NSI LAW AND POLICY PAPER

PRIVACY REGULATION AND **UNINTENDED CONSEQUENCES FOR SECURITY**

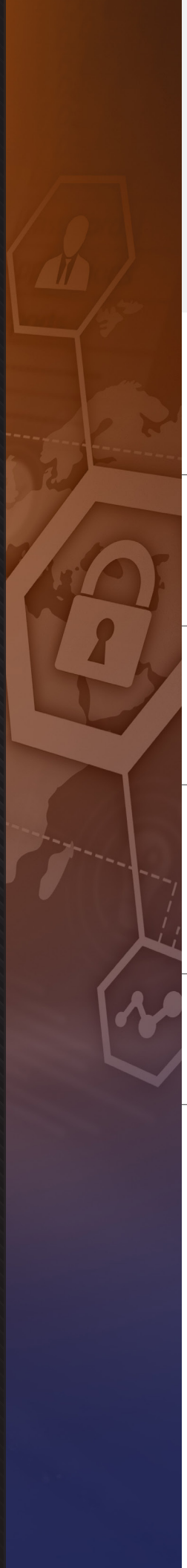
THIS NSI LAW AND POLICY PAPER:

1. Describes the federal urgency to act in response to public concern and the rapid global and domestic expansion of comprehensive privacy regulation.

2. Evaluates the implications privacy regulation can have for data protection and beneficial security activities.

3. Argues that AI, biometrics, and certain data categories are all critical to security innovations and activities and must be protected in privacy regulation.

4. Provides actionable recommendations to ensure privacy regulation appropriately balances individual rights with security.



CONTENTS

EXECUTIVE SUMMARY

Privacy Regulation Is Rapidly Expanding

GLOBAL & DOMESTIC PRESSURE IS MOUNTING TO PROTECT PERSONAL DATA

The extraordinary capacity to collect and harness data is leading governments around the world to provide greater protections for personal data. Europe's **Global Data Protection Regulation (GDPR)** served as a turning point for global tech companies by expanding the scope of protected personal data and granting individuals the rights to access and delete their data.

In the U.S., the Administration and Congress are now urgently seeking to respond to public concern and a proliferation of privacy regulation globally and among the states—most significantly, the recent **California Consumer Privacy Act (CCPA**).

Privacy Proposals Have Security Implications

EXPANSIVE DEFINITIONS OF PERSONAL DATA CAN LIMIT SECURITY ACTIVITY

Definitions of "personal data" or "personally identifiable information" (PII) have become expansive in the U.S. and abroad.

Expansive privacy protections can chill security work, as with the disruption GDPR created with the WHOIS tool, which makes domain name registrar information available and has long been an important tool for security and fraud prevention.

INDIVIDUAL RIGHTS TO CONTROL DATA CAN CREATE SECURITY ISSUES

Individual rights granted in privacy proposals include the ability to access, correct, transfer, or delete information, which can raise a range of security concerns. Risks include theft or exposure of data that has been centralized and made available for sharing, as well as the reduced quality of data sets needed for technologies like machine learning.

THREAT OF CLASS ACTIONS CAN STIFLE SECURITY WORK

Given the capacity of an alleged misstep with data and technology use to be widespread, it has particular potential to give rise to large classes of plaintiffs.

Recent litigation and legislative proposals have raised the prospect of class actions by plaintiffs based strictly on vulnerabilities. Without the occurrence of a concrete harm. This may create problematic disincentives as companies think twice about developing or deploying valuable innovations, including related to security tools or identity verification.

Authors' Views: Security Innovations Depend On Data And Must be Promoted

AI AND ROBUST DATA ARE CRITICAL TO SECURITY

Artificial intelligence (AI) will be central to advances in security, both in finding vulnerabilities and identifying key threats. Robust data is necessary for AI to evolve, and policymakers should avoid any disruption from privacy regulation and look instead to protect and expand available datasets.

BIOMETRICS SHOULD BE ENCOURAGED TO PROMOTE SECURITY

Technologists are looking beyond passwords to manage identity, and biometrics—from fingerprints to iris scans to facial images—are key security innovations to enhance security and public safety. Onerous privacy requirements can chill these security innovations.

VITAL DATA CATEGORIES NEED TO BE PROTECTED

Some data that could be considered "personal data" is vital to security, like IP addresses, Media Access Control (MAC) addresses, and location information. Some recent privacy efforts recognize that cyber activities use important personal data, but their narrow exceptions focus on necessity and should be broader.

Actionable Recommendations

1 AVOID OVERBROAD PII DEFINITIONS

Congress should avoid overbroad definitions of PII that would restrict beneficial security work or limit incentives for robust use of anonymized and aggregate data.

2 BALANCE INDIVIDUAL RIGHTS WITH SECURITY

Congress should ensure that access, correction, transfer, or deletion rights account for serious security concerns, such as cybersecurity information sharing, the use of AI security tools, and the risk of centralized or portable data sets.

3 ENSURE ROBUST SECURITY SAFE HARBORS

Congress should provide affirmative safe harbors and exceptions from liability that incentivize activities that are beneficial to the cyber ecosystem. Congress should also correct for the negative incentives created by liability for technical missteps that do not harm consumers.

4 DESIGN COLLABORATIVE, FLEXIBLE PRIVACY FRAMEWORKS

Congress should promote a predictable and flexible regulatory environment that promotes collaboration and adaptation, providing federal preemption, "cure" provisions, open collaboration with government enforcement authorities, and the use of voluntary standards.

PRIVACY REGULATION **IS RAPIDLY EXPANDING**

Global Pressure Is Mounting To Protect Personal Data

With the advent of the digital age and the growing awareness of the extraordinary capacity to collect and harness data for commercial uses, governments around the world are racing to provide greater protections for personal data.

- Europe's **Global Data Protection Regulation (GDPR)** created data protection requirements and gave Europeans strong individual control over the collection, use, and sharing of their personal information—leading companies to be careful about how they innovate and use this data.
- GDPR served as a turning point for global tech companies by expanding the scope of protected personal data, granting individuals the rights to access and delete their data, and defining what legitimate interests justify the use of consumer data.

States Are Driving Privacy Policy In The U.S.

All 50 states have enacted data breach notification laws[2] and many are now looking at far-reaching privacy laws.

- The most important so far is the **California Consumer Privacy Act (CCPA)**, which takes effect January 1, 2020 and is already influencing businesses.[3]
  - CCPA differs from the European Union's GDPR in certain respects, but similarly grants individuals control over their personal data, including rights to deletion and to opt out or deny the ability to sell personal information.[4]
- Other prominent efforts include the Washington Privacy Act (WPA), which was introduced in January 2019 and has a framework that mirrors GDPR,[5] as wells as Illinois' existing Biometric Information Privacy Act (BIPA),[6] which is having a growing impact as an expanding array of companies begin collecting biometric data from consumers, including fingerprints, iris scans, and facial recognition information.

Urgency to Act Is Mounting In Federal Government

Across the federal government, privacy is taking center stage as the Administration and Congress urgently seek to respond to public concern and catch up with a proliferation of privacy regulation both among the states and abroad.

- The National Telecommunications and Information Administration (NTIA) is leading a U.S. Commerce Department effort, coordinated with the National Economic Council (NEC),[7] to set a "broad outline of the direction that the Trump Administration should take to achieve U.S. consumer privacy protections."[8]
- The Commerce Department's National Institute of Standards and Technology (NIST) recently rolled out an effort "to develop a voluntary privacy framework to help organizations manage risk."[9]
- The Federal Trade Commission (FTC) is examining its authorities and takes an active role on privacy and data security enforcement—notably its recent record $5 billion settlement with Facebook,[10] while promoting best practices. FTC leadership has been calling for "Congress to enact privacy and data security legislation, enforceable by the FTC, which grants the agency civil penalty authority, targeted APA rulemaking authority, and jurisdiction over non-profits and common carriers."[11]
- In Congress, significant legislative proposals are beginning to take shape although a range of debates remain, including around the level of consumer control and the question of state preemption.

PRIVACY PROPOSALS HAVE **SECURITY IMPLICATIONS**

Expansive Definitions Of Personal Data Can Limit Security Activity

The most fundamental question in privacy policy is: what information deserves or requires protection? A key concept is "personal data" or "personally identifiable information" (PII), but definitions vary[12] and can be vague.

VAGUE AND BROAD DEFINITIONS OF PERSONAL DATA ARE BEING ADOPTED

There is no universal approach to PII in the United States or in the jurisdictions overseas that have adopted comprehensive privacy regulation.

- One federal agency defines it as "information that can be used to distinguish or trace an individual's identity ..., it requires a case-by-case assessment of the specific risk that an individual can be identified."[13]
- Some state definitions are expansive. California's CCPA defines "personal information" to cover everything from IP addresses to commercial information like records of personal property, products considered, biometric information, Internet browsing and search history, geolocation data, and audio, electronic, visual, thermal, and olfactory information.
- Likewise, Europe's GDPR defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject')."

EXPANSIVE DEFINITIONS CAN IMPACT SECURITY

Expansive privacy protections can chill security work and have unintended consequences, as with the impact of GDPR on the WHOIS tool.

- The WHOIS system makes the identifying and contact information of domain name registrars publicly available.
- WHOIS data has been an important tool for security and fraud prevention, and in tracking down bad guys on the Internet.
- The broad scope of GDPR has created document problems in administering this vital tool.

PRIVACY REGULATION AFFECTED WHOIS

WHOIS servers are a critical part of the functioning of the Internet and security activity. WHOIS services are run by registrars and registries. The ICANN organization coordinates a central registry for Internet resources, which includes references to the WHOIS servers of responsible registries as well as the contact details of the registries. Registries also maintain authoritative name servers, which identify websites' locations.[14]

The WHOIS function has been used by players across the ecosystem to facilitate security operations. But privacy regulations have created uncertainty impacting the utility and functionality of WHOIS services. "The impact of GDPR is being felt not only by businesses and individuals, but also by security researchers, investigators, and those who offer security products and services that rely on WHOIS data."[15]

"The GDPR requires that organizations collect only as much data as it needs for a specific business purpose, no more... Thanks to the uncertainty, some European DNS registrars have decided to no longer collect WHOIS information, for fear of drawing a hefty fine from regulators in an enforcement action."[16]

Individual Rights To Control Data Can Create Security Issues

INDIVIDUAL DATA RIGHTS ARE NOW BROAD

Prominent individual rights granted in privacy proposals include the ability to access, correct, transfer, or delete information about them.

- California's CCPA requires that businesses make information available in a useable format so a consumer can transmit data to another entity.
- Europe's "GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten.'"[17]

CONSUMER CONTROL CAN CREATE SECURITY VULNERABILITIES

These extensive individual rights over data can raise a range of security concerns.

- Questions around access and portability rights include how to securely transfer data to consumers. As privacy advocates like Electronic Frontier Foundation have explained, "[p]orted data can contain extremely sensitive

information..., and companies need to be clear about the potential risks before users move their data to another service."[18] Risks include theft or exposure of data that has been centralized for sharing, or transferring it to the wrong individual.

- Deletion of data can also affect the quality and breadth of underlying data sets, on which innovation and security will increasingly depend. Experts agree that good data is needed for technologies like machine learning.[19] If individuals or groups of individuals remove data from data sets, there may be impacts on the quality of data sets or the reliability of the outputs.
- For example, the permanent deletion of underlying records related to a particular user's activities—even where those activities are non-identifying or whether the data is fairly limited (e.g., metadata) could prevent the type of long-term analysis of behavioral trends that is increasingly used to identify new potential cybersecurity threats; this lack of historical data could create or perpetuate significant potential security vulnerabilities.

Threat Of Class Actions Can Stifle Security Work

Given the capacity of an alleged misstep with data and technology use to be widespread. Litigation risk and private rights of action have particular potential to give rise to large classes of plaintiffs and enormous damages.

A QUESTION OF HARM

Traditionally, privacy lawsuits have faced obstacles including the requirement of "standing" and actual harm. However, the status quo is changing as policymakers create private rights of action, as in the CCPA, and courts relax preconditions to sue.

- In *FCA v. Flynn*, a court certified a class action for claims that consumers paid too much for cars that were alleged to have later-discovered security vulnerabilities, despite no actual hack or breach. Amici urged the Supreme Court to hear the case, arguing that the plaintiffs had not been harmed and they did not have standing to sue.[20] The case is ongoing and more like it are coming.
- California legislators are considering expanding the CCPA's broad private right of action to make it easier to sue, and other states may follow suit.

A RISK TO SECURITY INNOVATIONS

The fear of class actions by plaintiffs without a concrete harm may create problematic disincentives impacting security.

- Companies may think twice about developing or deploying valuable innovations or novel data uses, including related to security tools or identity verification.

AUTHORS' VIEWS: **SECURITY INNOVATIONS DEPEND ON DATA AND MUST BE PROMOTED**

AI And Robust Data Are Critical To Security

AI WILL BE CENTRAL TO SECURITY ADVANCES

Artificial intelligence (AI) will be central to advances in security. "Just as cybersecurity analytics help to predict cyberattacks before they occur, AI techniques such as machine learning and deep learning can be used to find vulnerabilities that may be difficult for the security team to find."[21]

- As IBM explains, "[AI] is helping under-resourced security operations analysts stay ahead of threats. Curating threat intelligence from millions of research papers, blogs and news stories, AI provides instant insights to help you fight through the noise of thousands of daily alerts, drastically reducing response times."[22]

ROBUST DATA SETS ARE CENTRAL TO AI, AND SHOULD BE PROMOTED

Robust data is necessary for AI to evolve, and policymakers should look to protect and expand available datasets.

- When the White House announced its initiative to shape U.S. policy and support for AI it directed agencies to "improve data and model inventory documentation to enable discovery and usability" and to "prioritize improvements to access and quality of AI data and models."[23]
  - These provisions were designed to allow for broader access to AI data and models, and to allow for more robust use, analysis, and vetting of such data and models.
- Privacy regulation may disrupt data sets or limit access to data needed for AI. Classifications of data and restrictions on use should leave room for future data collection and analytics.

KEY TAKEAWAY

If companies are heavily regulated in their data acquisition and use, they may not create new data sets or mine existing ones, harming security innovation. If holders of data must delete data on request, data sets may be distorted and less useful. Policymakers should promote privacy without undermining innovation.

Use Of Biometrics Should Be Encouraged To Promote Security

BIOMETRICS CAN ENHANCE SECURITY

Technologists are looking beyond passwords to manage identity. NIST encourages multifactor authentication[24] and biometrics—from fingerprints to iris scans to facial images—are key factors.

- From smartphone thumbprint unlock to biometrics used in airport security, a wave of user-friendly methods can establish identity. Companies are using biometric tools to control facilities access. Facial analysis and recognition are used for public safety and security.

BIOMETRIC RULES CAN RESTRICT INNOVATION

Onerous privacy requirements can chill these security innovations.

- Illinois' biometric law is being used in hundreds of class actions to sue for millions of dollars from missteps in the collection of identifiers despite the absence of consumer harm.[25]
- Unreasonably punitive regimes can chill the development and use of beneficial tools.

KEY TAKEAWAY Biometrics deserve consideration for privacy, but overly strict regulation, or a presumption that use of biometrics is risky, may stifle their use and innovation.

Data Categories That Are Vital To Security Need Protecting

CERTAIN DATA WILL BE VITAL TO SECURITY

Some data that could be considered "personal data" is vital to security, like IP addresses, Media Access Control (MAC) addresses, and location information. "The IP address is used to transport data from one network to another network using the TCP/IP protocol. The MAC address is used to deliver the data to the right device on a network."[26]

- Websites and databases also use IP addresses and other information to facilitate secure access and identification. "IP address authentication is the traditional method of identifying users requesting access to vendor databases"[27] and a user's computer or site IP address can "eliminat[e] the need for user IDs and passwords."[28]
- In addition, the private sector, including third party security companies and aggregators, make use of location information for identity verification.
- The FTC has also noted that cross-device tracking offers benefits: "As more transactions move online, companies can determine if a consumer is using a new device to access an account and conduct additional authentication to ensure the account belongs to the consumer and not an impostor. Financial institutions often use this technique, which can reduce waste and fraud, and lower the likelihood of identity theft."[29]

SECURITY EXCEPTIONS ARE OFTEN NARROW OR ABSENT

Some recent privacy efforts recognize that cyber activities use important personal data, but their narrow exceptions focus on necessity and should be broader.

- CCPA has an exception from its consumer right to deletion, "if it is necessary for the business or service provider to maintain the consumer's personal information in order to .... Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity."[30]
- GDPR narrowly recognizes a legitimate basis to process some information for security purposes if it is "strictly necessary and proportionate" to "ensur[e] network and information security."[31]
- Prudent security measures may benefit from the use and maintenance of data, even if doing so is not what a lawyer may deem "necessary."

KEY TAKEAWAY

Some proposals restrict use of IP addresses, MAC addresses and location information, with potentially serious security consequences. Regulation should contain broad exceptions for uses related to security.

ACTIONABLE RECOMMENDATIONS

1 AVOID OVERBROAD PII DEFINITIONS

AVOID OVERBROAD DEFINITIONS OF PII THAT RESTRICT BENEFICIAL SECURITY WORK.

- Be wary of overly broad definitions of PII or categories of information that are subject to mandatory restrictions on collection, use, and sharing.
  - For example, the European Court of Justice's decision that IP addresses or similar data may be considered PII, under certain circumstances, makes such data potentially subject to GDPR provisions, including limitations on the use and retention of such data.[32]
  - Including information like IP and MAC addresses in PII or other protected categories may stifle important and beneficial security work and information sharing among private sector actors. The sharing of such data has been a cornerstone of federal cybersecurity policy for years, as reflected in the Cybersecurity Information Sharing Act of 2015.[33] Sharing cyber information is critical to staying ahead of threats and responding rapidly; fears of liability for sharing such data can slow down or stop sharing that is vital to modern cyber defense capabilities.
  - As such, policymakers should clarify and make explicit that such data is not subject to privacy protections or, to the extent it is, such protections are subject to an exception for cybersecurity purposes.
- Protect and expand incentives for anonymization, de-identification, and use of aggregate data.

2 BALANCE INDIVIDUAL RIGHTS WITH SECURITY

ENSURE THAT ACCESS, CORRECTION, TRANSFER, OR DELETION RIGHTS ACCOUNT FOR SERIOUS SECURITY CONCERNS

- Ensure that any consumer right to access, correct, delete or move data is narrow, practical, and based on reasonableness.
  - For example, as discussed above, the authorized deletion of data can cause significant cybersecurity

challenges. To the extent that data is being used for that purpose, it may be wise to consider an exception to standard data deletion provisions as set out below.

- Similarly, the right to modify data—unless it is actually incorrect—can undermine validity of an existing dataset and the ability of tools designed to understand and interpret data, which could lead to the creation of models and the development of analysis based on altered underlying data; to that end, it may be appropriate to limit authorized data modification to factual corrections for accuracy.

- Centralizing datasets and providing them to third parties is risky, and uniform formatting to enable portability may provide a roadmap for bad actors.
  - Policymakers should consider allowing flexibility in how datasets are stored, the format they utilize and what third-parties have access to them. This is important to limit the cybersecurity vulnerabilities inherent in significantly consolidating data sets in a single location, drastically expanding access to sensitive data, and using a single methodology for storage or formatting. Such flexibility can provide some measure of security through diversity.
- Consider rejecting or limiting the right to delete data, in order to preserve the accuracy of data sets on which innovation, research, and security tools are built.
  - Such a limitation might be focused on the beneficial objectives to be achieved by the collection, retention, and use of the data, including, as noted above, limitations on the right to delete data that is being used for cybersecurity purposes.

3 ENSURE ROBUST SECURITY SAFE HARBORS

INCLUDE SAFE HARBORS AND EXCEPTIONS FROM LIABILITY FOR SECURITY USES

- Promote security innovations that use data with broad exceptions for security uses and activities like private network management, security research, and database management.
  - Policymakers should not rely on a narrow "necessity" requirement, which can chill uses that would be helpful, if not strictly necessary.
  - Instead, exceptions focused on activities that are generally thought to be beneficial to the cyber ecosystem with fairly limited impact on personal privacy, should be affirmatively provided in any privacy law.
    - One example that might be useful for policymakers to examine is the broad affirmative authority provided for the collection, retention, and use of cyber threat information for cybersecurity purposes in the Cybersecurity Information Sharing Act of 2015.
- Correct for the negative incentives created by class action and other liability for technical missteps that do not harm consumers.

- Organizations need to be able to engage in beneficial security activities without uncertainty or liability risk.
- Policymakers should preserve existing constitutional standing requirements and promote a harm-based approach to enforcement and liability.
- Policymakers should also consider potential liability protection to incentivize certain beneficial activities, as did the limited liability protections for cybersecurity activities provided in the Cybersecurity Information Sharing Act of 2015.

4 DESIGN COLLABORATIVE, FLEXIBLE PRIVACY FRAMEWORKS

PROMOTE A PREDICTABLE AND FLEXIBLE REGULATORY ENVIRONMENT THAT PROMOTES COLLABORATION AND ADAPTATION

- **PREDICTABLE.** Champion national uniformity to help organizations innovate in a predictable environment and include preemption in any federal legislation. Preemption in this area can take different forms. Federal legislation can do more than create a regulatory "floor" on top of which states can layer additional divergent regulation. It can look at preempting private rights of action that may complicate and fragment legal expectations.
- **FLEXIBLE.** Include "cure" provisions that enable companies who make mistakes to fix them before being sued or facing enforcement actions. This is particularly important when it comes to any private rights of action.
- **COLLABORATIVE.** Encourage collaboration and advice by government enforcement authorities so that companies can seek guidance on how to comply with new expectations and operate in good faith to use reasonable and good faith practices.
  - One way to achieve such collaboration may be to provide a liability and regulatory free zone where companies can raise issues and obtain guidance without fear that the information shared or questions asked will lead to potential liability or enforcement actions.
- **ADAPTABLE.** Support the development of best practices by NIST and others, instead of static laws and regulations that are harder to modernize.
  - Given the challenges inherent in passing legislation and amending regulations, particularly in a rapidly changing technological environment, policymakers should instead consider providing clear guidance to agencies to encourage collaboration with industry—creating incentives for the use and implementation of best practices and advanced capabilities, and offering increased funding and authority to organizations like NIST that have strong collaborative relationships with industry that are able to make a substantive impact on these issues without mandating specific requirements.

ENDNOTES

1 Megan Brown is a Senior Fellow and Associate Director of Cybersecurity at the National Security Institute at the Antonin Scalia Law School at George Mason University. Ms. Brown is currently a partner in Wiley Rein LLP's Telecom, Media & Technology and Privacy & Cybersecurity practices. She previously served in the Department of Justice as Counsel to two U.S. Attorneys General. James Burchfield is a Visiting Fellow at the National Security Institute at the Antonin Scalia Law School at George Mason University. Mr. Burchfield is also a partner at Williams & Jensen. Prior to joining Williams & Jensen, Mr. Burchfield served as a Congressional staffer on the House Foreign Affairs Committee and the House Small Business Committee.

James B. Burchfield is currently a Visiting Fellow at the National Security Institute. James is also a partner at Williams & Jensen where he is responsible for managing a variety of issues for clients including foreign policy, data privacy and cybersecurity issues. Prior to his work at Williams & Jensen, James served as a Congressional staffer on the House Foreign Affairs Committee and the House Small Business Committee. He also functioned as a Senior Policy Adviser to a senior Member of Congress where he led the strategic policy agenda on foreign policy and judiciary issues. He earned his bachelor's degree in economics and international affairs from Loyola University of Chicago and has received executive education from Harvard University's John F. Kennedy School of Government in trade policy.

2 Lothar Determann, *Broad data and business regulation, applicable worldwide*, Int'l Assoc. of Privacy Prof'ls, Inc. (July 2, 2018), https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/.

3 Cal. Civ. Code § § 1798.100 to .198 (2018).

4 Nancy Libin & Rachel R. Marmor, *Washington Privacy Act, as Introduced in the Washington Legislature: A Rapid Q&A*, Lexology (Feb. 6, 2019), https://www.lexology.com/library/detail.aspx?g=0db4459d-82be-43c1-9888-a2ca1e32ced4.

5 National Telecommunications and Information Administration, *Request for Comments on Developing the Administration's Approach to Consumer Privacy*, U.S. Dep't of Commerce (Sept. 25, 2018), https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy.

6 740 Ill. Comp. Stat. 14 / 1 (2008).

7 National Telecommunications and Information Administration, *NTIA Seeks Comment on New Approach to Consumer Data Privacy*, U.S. Dep't of Commerce (Sept. 25, 2018), https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy.

8 National Institute of Standards and Technology, Department of Commerce Launches Collaborative Privacy Framework Effort (Sept. 4, 2018), https://www.nist.gov/news-events/news/2018/09/department-commerce-launches-collaborative-privacy-framework-effort.

9 *Hearing on "Oversight of the Federal Trade Commission: Strengthening Protections for American's Privacy and Data Security" Comm. on Energy and Commerce Sub. Comm. on Consumer Protection and Commerce*, 166th Cong. (2019) (prepared remarks of Chairman Joseph J. Simmons) https://www.ftc.gov/system/files/documents/public_statements/1519226/2019_ec_oral_remarks.pdf.

10 Federal Trade Commission, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

11 Privacy Act of 1974 U.S.C. § 552a (1974).

12 General Services Administration, *Rules and Policies - Protecting PII - Privacy Act* (Oct. 31, 2014), https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act.

13 Information Commissioners Office, *Right to Erasure*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/.

14 ICANN WHOIS, *DNS and WHOIS- How it Works*, Internet Corporation for Assigned Names and Numbers, https://whois.icann.org/en/dns-and-whois-how-it-works.

15 Kevin Rollinson, *GDPR and WHOIS: Here's What You Need to Know*, Cisco Umbrella (May 31, 2018), https://umbrella.cisco.com/blog/2018/05/31/gdpr-and-whois/.

16 Tara Seals, *ICANN Launches GDPR Lawsuit to Clarify the Future of WHOIS*, ThreatPost (May 31, 2018), https://threatpost.com/icann-launches-gdpr-lawsuit-to-clarify-the-future-of-whois/132427/.

17 Gene Gebhart, Bennet Cyphers, & Kurt Opsahl, *What We Mean When We Say "Data Portability,"* Electronic Frontier Foundation (Sept. 13, 2018), https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability.

18 Maria Korolov, *AI's biggest risk factor: Data gone wrong*, CIO MAGAZINE (Feb. 13, 2018, 3:00 PM), https://www.cio.com/article/3254693/ais-biggest-risk-factor-data-gone-wrong.html. "Collecting, classifying and labeling datasets used to train the algorithms is the grunt work that's difficult — especially datasets comprehensive enough to reflect the real world." *Id.*

19 NEC, *AI for Cyber Security: How AI prevents future cyberattacks?* (Oct. 6, 2016), https://www.nec.com/en/global/ad/insite/article/safety10.html.

20 Brief for FCA US LLC & Harman Int'l Indus. as Amicus Curiae Supporting Petitioners, FCA US LLC & Harman Int'l Indus. v. Flynn 327 F.R.D. 206 (2018) (No. 18-398).

21 IBM, *Artificial intelligence for a smarter kind of cybersecurity*, https://www.ibm.com/security/artificial-intelligence.

22 Id.

23 Exec. Order No. 13859, 3 C.F.R. (Feb. 11, 2019).

24 National Insitute of Standards and Technology, *Digital Identity Guidelines: Now Available*, SP 800-63-3 (Jun. 22, 2017), https://doi.org/10.6028/NIST.SP.800-63-3.

25 *See* Rosenbach v. Six Flags Entertainment Corp., No. 2-17-0317, 2017 Ill. App. (2d) 170317, http://www.illinoiscourts.gov/Opinions/SupremeCourt/2019/123186.pdf (finding that a plaintiff can be "aggrieved" so that they can "seek liquidated damages and injunctive relief pursuant to [state law]" even "if he or she has not alleged some actual injury or adverse effect, beyond violation of his or her rights under the statute.").

26 EBSCOConnect, *What is the correct syntax for an EBSCOhost or EBSCO Discovery Service Persistent Link?* (July 15, 2019), http://eadmin.epnet.com/eadmin/help/authentication/IP_Address_Auth.*Id.*

27 *Id.*

28 *Id.*

29 Federal Trade Commission, *Cross Device Tracking* (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf. Consolidated Appropriations Act, Pub. L. No. 114-113, 129 Stat. 2242, 2936 (codified at 6 U.S.C. §§ 1501-1510).

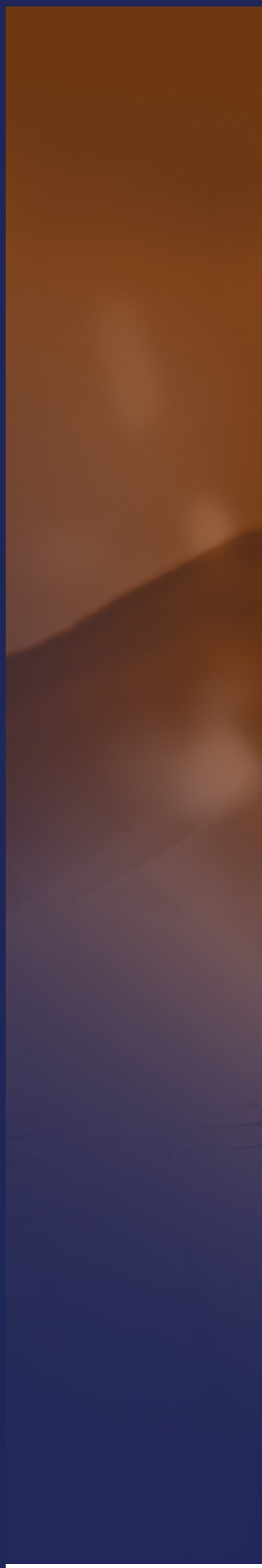
30 2018 Cal. ALS 55 (LexisNexis).

31 2016 O. J. (L 119) 680.

32 C-582/14, Breyer v. Bundesrepublik Deutschland, 2C.M.L.R. 81 (2017).

33 Cybersecurity Information Sharing Act, 6 U.S.C.S. § 1502 (LexisNexis 2015).

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



THE NATIONAL SECURITY INSTITUTE
Antonin Scalia Law School | George Mason University
3301 Fairfax Dr. Arlington, VA 22201 | 703-993-5620

NATIONALSECURITY.GMU.EDU