GENERAL COMMITTEE MEETING

Thursday, October 25, 2018

3:00 PM to 4:00 PM

Healthcare Leadership Council

750 9th Street, NW, Suite 500 Washington, D.C. 20001

Conference Line: 888-432-1688, Room: 6597, User: 6328

1. **Welcome and Introductions**
2. **Fall Unified Agenda: Guest Speaker, Jenn Geetter, McDermott Will & Emery**
    a. **HIPAA Privacy: Request for Information on Changes to Support, and Remove Barriers to, Coordinated Care**
    b. **HIPAA Enforcement: Sharing Civil Money Penalties or Monetary Settlements**
    c. **HIPAA Privacy Rule: Presumption of Good Faith of Health Care Providers**
3. **Accounting of Disclosures Survey**
4. **Senate Commerce Committee Update**
5. **NTIA Request for Comment**
6. **NIST Collaborative**
7. **California Consumer Privacy Act of 2018**

8. General Data Protection Regulation

Next meeting: Thursday, November 15, 2018 at 3:00 PM

RIN Data

HHS/OCR **RIN:** 0945-AA00 **Publication ID:** Fall 2018

Title: HIPAA Privacy: Request for Information on Changes to Support, and Remove Barriers to, Coordinated Care

Abstract:

This Request for Information (RFI) would solicit the public's views on whether there are provisions of the HIPAA Rules which present barriers that limit or discourage coordinated care and case management among hospitals, physicians (and other providers), payors, and patients, or otherwise impose regulatory burdens that may impede the transformation to value-based health care without providing commensurate privacy or security protections for patients' protected health information and while maintaining patients' ability to control the use or disclosure of their PHI and to access PHI. In addition to a general request for information, the RFI would specifically seek comment on a number of particular issues, including: (1) Methods of accounting of all disclosures of a patient's protected health information; (2) patients' acknowledgment of receipt of a providers' notice of privacy practices; (3) creation of a safeharbor for good faith disclosures of PHI for purposes of care coordination or case management; (4) disclosures of protected health information without a patient's authorization for treatment, payment, and health care operations; (5) the minimum necessary standard/requirement. This RFI would subsume the previous 0945-AA08 entry in the Regulatory Agenda.

Agency: Department of Health and Human Services(HHS)

Priority: Other Significant

RIN Status: Previously published in the Unified Agenda

Agenda Stage of Rulemaking: Prerule Stage

Major: Undetermined

Unfunded Mandates: Undetermined

EO 13771 Designation: Other

CFR Citation: 45 CFR 164

Legal Authority: Pub. L. 115-5, sec. 13405(c)

Legal Deadline:

Action	Source	Description	Date
Final	Statutory	The statutory deadline to issue a rule on accounting of disclosures was 06/01/2010	06/01/2010

Overall Description of Deadline: Required by the HITECH Act. Statutory deadline contingent on further regulatory action.

Statement of Need:

The HHS Deputy Secretary recently launched an initiative called the Regulatory Sprint to Coordinated Care. The goal of the Regulatory Sprint is to remove regulatory barriers that impede coordinated, value-based health care. This RFI is being produced to support the Regulatory Sprint.

Summary of the Legal Basis:

The HIPAA statute and its amendments.

Alternatives:

None were considered as this RFI is intended to solicit various policies for improving HIPAA.

Anticipated Costs and Benefits:

No anticipated costs as this is not regulatory. Benefits include receiving public feedback on potential policies to pursue in rulemaking.

Risks:

None known.

Timetable:

Action	Date	FR Cite

NPRM	05/31/2011	76 FR 31426
NPRM Comment Period End	08/01/2011	
NPRM Withdrawal	11/00/2018	
RFI	11/00/2018	

Regulatory Flexibility Analysis Required: Undetermined

Government Levels Affected: Undetermined

Federalism: No

Included in the Regulatory Plan: Yes

RIN Information URL: www.hhs.gov/ocr/privacy

RIN Data Printed in the FR: No

Agency Contact:
Andra Wicks
Health Information Privacy Specialist
Department of Health and Human Services
Office for Civil Rights
200 Independence Avenue SW,
Washington, DC 20201
Phone:202 774-3081
TDD Phone:800 537-7697
Email: andra.wicks@hhs.gov

RIN Data

HHS/OCR **RIN:** 0945-AA09 **Publication ID:** Fall 2018

Title: HIPAA Privacy Rule: Presumption of Good Faith of Health Care Providers

Abstract:

In an effort to address the opioid epidemic, the proposed rule would make a number of changes to provisions of the HIPAA Privacy Rule regarding uses and disclosures of protected health information to ease the burden on and potential risks to covered entities that may want to disclose PHI in such circumstances.

Agency: Department of Health and Human Services(HHS)

Priority: Other Significant

RIN Status: Previously published in the Unified Agenda

Agenda Stage of Rulemaking: Proposed Rule Stage

Major: No

Unfunded Mandates: No

EO 13771 Designation: Deregulatory

CFR Citation: 45 CFR 164.510

Legal Authority: Health Insurance Portability and Accountability (HIPAA) Act of 1996, Pub. L. 104-191

Legal Deadline: None

Statement of Need:

With over 60,000 individuals dying of opioid overdoses in 2016 and others suffering from addiction to the opiates, HHS issued a declaration of emergency to recognize a nationwide opioid epidemic. HIPAA permits providers and other covered entities to disclose protected health information about an individual to families, caregivers and other relevant parties in circumstances related to opioid overdose and addiction. Despite this permission and HHS guidance clarifying HIPAA, HHS continues to receive anecdotal evidence that providers and other covered entities are reluctant to share an opioid patient's health information with family or other caregivers.

This proposal seeks to encourage covered entities to share protected health information with family members, caregivers, and others in a position to avert threats of harm to health and safety when necessary to promote the health and recovery of those struggling with opioid addiction.

Summary of the Legal Basis:

OCR has broad authority under the HIPAA statute to make modifications to the Privacy Rule, within the statutory constraints of HIPAA, the HITECH Act, and other applicable law (e.g., the Administrative Procedures Act).

OCR, by delegation from the Secretary, has broad authority under HIPAA to make modifications to the Privacy Rule, as provided by section 264 of HIPAA (codified at 42 U.S.C. 1320d-2(note)).

Alternatives:

OCR may issue additional guidance as an alternative to the proposed rule. However, HIPAA continues to be cited as a barrier to sharing protected health information in crisis situations, despite extensive existing guidance and outreach efforts. Without regulatory changes, it is not clear that additional guidance would be effective in clarifying the ability to share protected health information in such situations. Revising the Privacy Rule would be a more effective and permanent vehicle for achieving the desired policy, and would provide additional Good Samaritan safe harbor protections to health care providers who share protected health information when trying to help patients.

Anticipated Costs and Benefits:

The proposed rule will not create any new requirements or costs for regulated entities or the public. It will benefit patients and families by helping to ensure that family members and others involved in the patients' care can get the information they need to help their loved ones obtain appropriate care and support. It will also provide additional

protections to health care providers exercising their professional judgment when making disclosures of protected health information to further the interests of patients.

Risks:

While we do not anticipate significant risks to privacy associated with this proposal, the NPRM requests public input on whether the impact of these amendments, taken together, could be expected to discourage individuals from seeking care based on concerns that their PHI may be disclosed against their wishes.

Timetable:

Action	Date	FR Cite
NPRM	01/00/2019	

RIN Data

HHS/OCR **RIN:** 0945-AA04 **Publication ID:** Fall 2018

Title: HIPAA Enforcement: Sharing Civil Money Penalties or Monetary Settlements

Abstract:

This Request for Information (RFI) would solicit the public's views on the distribution and disclosure of civil money penalty or monetary settlements shared with those harmed by a Health Insurance Portability and Accountability Act (HIPAA) offense.

Agency: Department of Health and Human Services(HHS)

Priority: Other Significant

RIN Status: Previously published in the Unified Agenda

Agenda Stage of Rulemaking: Prerule Stage

Major: No

Unfunded Mandates: No

EO 13771 Designation: Other

CFR Citation: 45 CFR 160

Legal Authority: Pub. L. 111-5, sec. 13410(c)(3)

Legal Deadline:

Action	Source	Description	Date
Final	Statutory	The statutory deadline for issuing a rule on civil monetary penalties was 2/1/2012.	02/01/2012

Timetable:

Action	Date	FR Cite
Request For Information (RFI)	01/00/2019	

Regulatory Flexibility Analysis Required: No

Government Levels Affected: None

Small Entities Affected: No

Federalism: No

Included in the Regulatory Plan: No

RIN Information URL: www.hhs.gov/ocr/privacy

RIN Data Printed in the FR: No

Agency Contact:

Andra Wicks
Health Information Privacy Specialist
Department of Health and Human Services
Office for Civil Rights
200 Independence Avenue SW,
Washington, DC 20201
Phone:202 774-3081
TDD Phone:800 537-7697
Email: andra.wicks@hhs.gov

Accounting of Disclosures Calculation of the Impact of New Privacy Rule Requirements

Current Law

Under current HIPAA privacy rules (45 CFR §164.528), individuals have a right to receive within 60 days of the request (with one 30 day extension available) an accounting of disclosures of their protected health information (PHI) made by a covered entity (CE), including disclosures to or by the CE's business associates (BA) for up to six years prior to the date on which the accounting is requested, except for disclosures:

1 for treatment, payment, or health care operations
2 to the individual or his personal representative
3 incident to otherwise permitted or required uses or disclosures
4 pursuant to an authorization
5 for the facility's directory or to persons (e.g. family members) included in the person's care and for disaster relief
6 for national security or intelligence purposes
7 to correctional institutions or law enforcement officials for certain purposes
8 of a limited data set
9 that occurred prior to the compliance date for the CE

For each disclosure, the following must be provided:

1 the date of the disclosure
2 the name of the entity or person who received the PHI and, if known, the address
3 a brief description of the PHI disclosed
4 a brief statement of the purpose of the disclosure or a copy of the request for the disclosure

Multiple disclosures to the same entity or person may be aggregated. For disclosures for research of the PHI of more than 50 individuals the CE may provide summary information about the disclosures (which may or may not include the requesting individual's PHI) and contact information for the researcher and the research sponsor. CEs must provide the first accounting of disclosures report without charge. Reasonable cost-based fees may be imposed for additional requests by the same individual within the 12-month period provided the CE informs the individual in advance of the fee and provides an opportunity for the individual to withdraw or modify the request.

Responding to Requests for an Accounting of Disclosures Report Under Current Law (this information will help assess the current compliance burden and the current level of individuals' interest in accounting of disclosures reports):

1. Approximately how many patients do you annually provide care for, pay claims for, or otherwise serve? _____
2. (a) How many individuals have requested an accounting of disclosures report since 2010?_____
   (b) How many individuals requested an accounting of disclosures report in 2017? _____
3. How many disclosures (please provide an average and/or a range) were listed in the reports you produced? _____
4. How many of the disclosures listed in the reports you produced were for research purposes (average and/or range please)?
_____
5. Generally describe the steps taken to generate an accounting of disclosures report: _____
_____
6. Does your staff proactively document the information specifically required for the report at the time a disclosure is made or do you only retroactively recreate/extract this information from existing documentation at the time a patient requests a report?
_____
7. How many information systems with PHI do you have? _____
8. How many information systems are searched to produce a report? _____
9. (a) How many automated system interfaces do you have that convey PHI between systems (please describe)? _____
   (b) How many of these interfaces convey PHI between separate covered entities? _____
   (c) How many interfaces do you have with Business Associates (please describe)?_____
10. (a) How many authorized users do your information systems with PHI have? _____ (b) Of these authorized users, how many are employed by you or considered part of your workforce? _____ (c) Of these authorized users, how many are affiliated, credentialed providers (e.g., non-employed physicians with privileges at your facility)? _____
11. How many of your information systems currently store audit trail data?_____
12. What elements do your audit trails capture (user id, log on/off, date/time stamp, patient id, description of information accessed, etc)?
_____ _____
13. How long do your audit trails hold information? _____
14. Do your audit trails distinguish between a use and disclosure? If so, how? ?_____
15. (a) Describe how audit trails were utilized to produce the report, if at all? _____ (b) What, if anything, in addition to audit trails, was used to produce the report?_____
_____
16. Approximately how many professional staff hours are needed to compile the report (please provide an average and/or a range)?_____
17. What is the average cost and/or the range of costs incurred to produce a report? _____ _____
_____
18. If known, what prompted individuals to request an accounting of disclosures report? _____
19. Were the requestors satisfied with the accounting of disclosures report? _____

Impact of Expanded Accounting of Disclosures Requirements to Include Disclosures Relating to Treatment, Payment, and Health Care Operations

The HITECH Act, part of the American Recovery and Reinvestment Act of 2009 (the stimulus package), was signed into law by President Obama on February 17, 2009. **Section 13405(c) of the Act newly requires CEs that use or maintain an Electronic Health Record (EHR)[i] to provide, upon request, an accounting of disclosures[ii] made for treatment, payment and health care operations[iii] purposes through an EHR over a three-year period.** In response to a request, CEs may either provide an accounting for disclosures of PHI made by the CE and its business associates or may provide an accounting of disclosures made by the CE and a list of all BAs acting on behalf of the CE including contact information for the BAs. BAs on a CE's list must, in response to a request, provide an accounting of its disclosures.

To calculate the impact of this requirement on Covered Entities and their Business Associates:

1. Is your organization a Covered Entity? If yes, what type of Covered Entity (plan, provider, OHCA, etc) and how many business associates do you have? _____
2. Is your organization a business associate? If yes, please describe your organization: _____
3. Approximately how many disclosures for treatment purposes are made annually?_____
4. Approximately how many disclosures for payment purposes are made annually? _____
5. Approximately how many disclosures for health care operations purposes are made annually?_____
6. The Privacy Rule currently requires that an accounting of disclosures report include the date of the disclosure, a description of the information disclosed, the name (and if known the address) of the entity or person who received the information disclosed, and a statement of the purpose for the disclosure or a copy of the written request for the disclosed information. Anticipating that expanded reporting for treatment, payment and healthcare operations purposes would be similar to current reporting, do you currently have the capacity to produce an accounting of disclosures report that includes such information? _____
7. Would additional storage capacity be required to maintain three years of data on disclosures for treatment, payment and health care operations? _____
   a. If yes, how much additional storage capacity would be required? _____
   b. If yes, what would be the cost of adding this additional storage capacity? _____
8. Would additional programming capacity or infrastructure be required to capture and maintain three years of data on disclosures for treatment, payment and health care operations?_____
   a. If yes, how much additional programming capability would be required?_____
   b. If yes, what would be the cost be of adding this additional capacity? _____
9. Would additional personnel be needed to maintain the capacity to produce accounting of disclosures reports that included disclosures for treatment, payment and health care operations over a three-year period?_____
   a. If yes, how much additional personnel would be needed? _____
   b. If yes, what would be the cost of adding this additional capacity?_____
10. What would you suggest to ease the compliance burden? (e.g., reduce the information required to be collected about each disclosure/eliminate the requirement to account for disclosures made to health care providers who are authorized users of the CEs EHR/allow CEs to charge for the labor cost of creating a report)

_____

_____

11. a. What is the approximate total cost of altering your operations to be able to comply with the expanded accounting of disclosures requirements?_____
    b. How long do you estimate it will take to make these changes to your systems? _____
    c. What is the estimated annual cost of system maintenance? (just the incremental cost for compliance with the new requirements)

_____

    d. How many man hours do you estimate it would take to compile an accounting of disclosures report only for disclosures for treatment, payment and health care operations disclosures? _____

Your Name & Title: _____

Company: _____

Address:_____

Phone Number & Email Address:_____

[1] ***Electronic Health Record*** means an "electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff." **(**HITECH Act §13400(5)) [1] ***Disclosure*** means "the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information." This is different from "***use***," which means, "with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information." (45 CFR 160.103) [1] ***Treatment*** means the provision, coordination, or management of healthcare and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. (45 CFR 164.501) ***Payment*** means*:* (1)The activities undertaken by: (i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and (2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to: (i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; (ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics; (iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related healthcare data processing; (iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement: (A) Name and address; (B) Date of birth; (c) Social security number; (D) Payment history; (E) Account number; and (F) Name and address of the healthcare provider and/or health plan. (45 CFR 164.501) ***Health care operations*** means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; (3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable; (4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; (5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and (6) Business management and general administrative activities of the entity, including, but not limited to: (i) Management activities relating to implementation of and compliance with the requirements of this subchapter; (ii) Customer service, including the provision of data analyses for policyholders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer. (iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and (v) Consistent with the applicable requirements of §164.514, creating deidentified health information or a limited data set, and fundraising for the benefit of the covered entity. (45 CFR 164.501)

MeriTalk
Improving the Outcomes of Government IT

Senate Commerce Eyes GDPR, CCPA Amid Push for Data Privacy Law

Oct 10, 2018 | 12:38 pm

The Senate Commerce, Science, and Transportation Committee heard testimony today detailing the workings of data privacy laws in Europe and California–specifically the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)–amid a growing groundswell for Congress to work on a national data privacy law for the U.S.

When the committee held a hearing met last month featuring technology companies and internet service providers, committee Chairman Sen. John Thune, R-S.D., made a point to mention that the industry will not write Federal data privacy legislation, and that the industry cannot be trusted to regulate itself.

"A national standard for privacy rules of the road is needed to protect consumers," he said.

Sen. Edward Markey, D-Mass., filling in for committee Ranking Member Bill Nelson, D-Fla., who was returning to his home state ahead of Hurricane Michael, said he was glad that during last month's hearing AT&T, Amazon, Google, Twitter, Apple, and Charter Communications all agreed that Federal data privacy regulations are needed.

However, he said senators shouldn't be under any "delusions" as to why tech companies are suddenly on board with Congress taking action on data privacy, and credited companies having to conform to GDPR and CCPA for the industry's change of heart.

Andrea Jelinek, chair of the European Data Protection Board, unsurprisingly, stressed the importance of regulation in her testimony.

"The volume of digital information in the world doubles every two years, artificial intelligence systems and data processing deeply modify our way of life and the governance of our societies," she said. "If we do not modify the rules of the data processing game with legislative initiatives, it will turn into a losing game for the economy, society and for each individual."

Both Jelinek and Alastair Mactaggart, chair of Californians for Consumer Privacy, discussed the basic principles that form the foundation of GDPR and CCPA.

For Jelinek, it was putting individuals at the center of privacy practices, accountability, and using a risk-based approach to data collection. Mactaggart similarly explained that CCPA is based on transparency, control, and accountability. Essentially, both pieces of legislation prioritize the individual's right to know what information is being collected and how it will be used, while also making those collecting data responsible for securing and using the information responsibly.

Both Jelinek and Mactaggart addressed concerns that privacy laws will hurt businesses and will stymie innovation–arguments frequently leveled by those opposed to stricter data privacy regulations.

"It is often said that the U.S. approach to data protection promotes technological innovation and economic growth, which is important for people living on both sides of the Atlantic," Jelinek said. "Let me give you my opinion on that: without trust, there is no economic growth and no innovation at the end of the day. Companies should be allowed to continue to use and share data, as long as they do so in a transparent and lawful manner, respecting the rights of individuals."

"CCPA is not anti-business," said Mactaggart. "It was, on the contrary, written and proposed by businesspeople concerned that regulations were needed; that as in so many previous situations, whether of the giant trusts of a century and more ago, or of the telephone and related wiretapping concerns, or cigarettes and health, or autos and safety, this latest technology too, has outpaced society's ability to fully comprehend it yet, or its impact on all of us."

Laura Moy, executive director at the Center on Privacy & Technology at Georgetown Law, had a different perspective on the importance of data privacy. While other witnesses focused on the importance of data privacy for the individual, Moy focused on the societal implications of unregulated data collection.

"This is about our country–and the world–grappling with the implications of unbridled data collection, storage, and use–things that give the holders and users of data more power to influence society than we could have imagined before the digital era," she said. "This is about confronting the ways in which the data-driven economy is contributing to extreme wealth disparity, extreme political polarization, extreme race- and class-based tension, and extreme information manipulation. We need to come together to rein in the problematic ways in which Americans' data is being collected and stored without meaningful limitations, and used in ways that harm not only individuals, but our broader society."

While her perspective may have differed from the other witnesses, the six recommendations Moy offered to the committee closely aligned with their basic policy prescriptions.

Moy stressed that: there are appropriate and inappropriate collections and uses of Americans' information; privacy protections should be strongly enforced by an expert Federal agency; privacy protections should also be enforced by state attorneys general; privacy and data security protections should be forward-looking and flexible; protections for Americans' private information should take into account the context in which information is shared; and Congress should not eliminate existing protections for Americans' information.

Nuala O'Connor, president and CEO of the Center for Democracy & Technology, agreed with Moy's recommendations and stressed in her testimony the importance of regulation and enforcement on a Federal and state level.

"Instead of relying primarily on privacy policies and other transparency mechanisms, Congress should create an explicit and targeted baseline level of privacy protection for individuals," she said. "[L]egislation should enshrine basic individual rights with respect to personal information; prohibit unfair data processing; deter discriminatory activity and give meaningful authority to the FTC [Federal Trade Commission] and state attorneys general to enforce the law."

Department of Commerce Launches Collaborative Privacy Framework Effort

NIST Will Hold Public Workshop on Oct. 16, 2018

September 04, 2018

GAITHERSBURG, Md. – Innovative technologies such as the “internet of things” (IoT) and artificial intelligence enhance convenience, efficiency and economic growth. At the same time, these and other technologies increasingly require complex networking environments and use detailed data about individuals that can make protecting their privacy harder.

To help meet this challenge, the U.S. Department of Commerce’s National Institute of Standards and Technology (NIST) announced today that it has launched a collaborative project to develop a voluntary privacy framework to help organizations manage risk.

“We’ve had great success with broad adoption of the NIST Cybersecurity Framework, and we see this as providing complementary guidance for managing privacy risk,” said Under Secretary of Commerce for Standards and Technology and NIST Director Walter G. Copan. “The development of a privacy framework through an open process of stakeholder engagement is intended to deliver practical tools that allow continued U.S. innovation, together with stronger privacy protections.”

The envisioned privacy framework will provide an enterprise-level approach that helps organizations prioritize strategies for flexible and effective privacy protection solutions so that individuals can enjoy the benefits of innovative technologies with greater confidence and trust.

Parallel with this effort, Commerce’s National Telecommunications and Information Administration is developing a domestic legal and policy approach for consumer privacy in coordination with the department’s International Trade Administration to ensure consistency with international policy objectives.

To collect input from stakeholders, NIST will kick off the effort with a public workshop on Oct. 16, 2018, in Austin, Texas—in conjunction with the International Association of Privacy Professionals’ Privacy. Security. Risk. 2018 conference.

Good cybersecurity practices are central to managing privacy risk but are not sufficient. According to NIST's description of the new project, organizations need access to additional tools to better address the full scope of privacy risk.

“Consumers’ privacy expectations are evolving at the same time that there are multiplying visions inside and outside the U.S. about how to address privacy challenges,” said NIST Senior Privacy Policy Advisor and lead for the project, Naomi

Lefkovitz. “NIST’s goal is to develop a framework that will bridge the gaps between privacy professionals and senior executives so that organizations can respond effectively to these challenges without stifling innovation.”

The Austin public workshop is the first in a series planned to collect current practices, challenges and needs in managing privacy risks in ways that go beyond common cybersecurity practices.

Over the coming year, through these workshops and other outreach efforts, said Lefkovitz, “we want to gather the best ideas from many stakeholders so that the privacy framework tool we develop is useful and effective for a wide range of organizations.”

NIST has also posted an overview of the development schedule for this framework. To learn more, and to register for the Austin public workshop, visit the event website by Oct. 9, 2018.

The workshop will be recorded and shared on the Privacy Framework website.

NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life. NIST is a non-regulatory agency of the U.S. Department of Commerce. To learn more about NIST, visit www.nist.gov.

NIST Privacy Framework

An Enterprise Risk Management Tool

Why a Privacy Framework

The challenge

It is a challenge to design, operate, or use technologies in ways that are mindful of diverse privacy needs in an increasingly connected and complex environment. Inside and outside the U.S., there are multiplying visions for how to address these challenges.

Why good cybersecurity doesn't solve it all

While good cybersecurity practices help manage privacy risk by protecting people's information, privacy risks also can arise from how organizations collect, store, use, and share this information to meet their mission or business objective, as well as how individuals interact with products and services.

Addressing the privacy challenge

The U.S. Department of Commerce is developing a forward-thinking approach that supports innovation and strong consumer privacy protections. The National Institute of Standards and Technology (NIST) is leading the development of a voluntary privacy framework as an enterprise risk management tool for organizations while the National Telecommunications and Information Administration is leading the development of a set of privacy principles, and coordinating with the International Trade Administration to ensure consistency with international policy objectives.

What is the NIST Privacy Framework

- NIST aims to collaboratively develop the Privacy Framework as a voluntary, enterprise-level tool that could provide a catalog of privacy outcomes and approaches to help organizations prioritize strategies that create flexible and effective privacy protection solutions, and enable individuals to enjoy the benefits of innovative technologies with greater confidence and trust.
- It should assist organizations to better manage privacy risks within their diverse environments rather than prescribing the methods for managing privacy risk.
- The framework should also be compatible with and support organizations' ability to operate under applicable domestic and international legal or regulatory regimes.

NIST's Collaborative Process

- NIST has a long track record of successfully and collaboratively working with the private sector and federal agencies to develop guidelines and standards. With experience in developing the *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) and extensive privacy expertise, NIST is well positioned to lead the development of this framework.
- NIST will model the approach for this framework based on the successful, open, transparent, and collective approach used to develop the Cybersecurity Framework.
- NIST will convene and work with industry, civil society groups, academic institutions, Federal agencies, state, local, territorial, tribal, and foreign governments, standard-setting organizations, and others, conducting extensive outreach through a series of workshops and requests for public comment.

CONTACT | privacyframework@nist.gov
LEARN MORE | Visit www.nist.gov/privacyframework

BROOKINGS

QUALITY. INDEPENDENCE. IMPACT.

Developing the NIST Privacy Framework: How can a collaborative process help manage privacy risks?

The Brookings Institution
Monday, September 24, 2018
9:00 a.m. – 12:00 p.m.

BROOKINGS

EVENT ANNOUNCEMENT

Developing the NIST Privacy Framework: How can a collaborative process help manage privacy risks?

Monday, September 24, 2018, 9:00 a.m. — 12:00 p.m.

The Brookings Institution, Falk Auditorium, 1775 Massachusetts Ave, NW, Washington, DC

The "Cybersecurity Framework" led by the National Institute of Standards and Technology (NIST) has proved to be a valuable tool of cybersecurity risk management. Now, with privacy in the public spotlight and discussions about policy options expanding, NIST is embarking on a collaborative effort to develop a NIST "Privacy Framework: An Enterprise Risk Management Tool."

On September 24, the Center for Technology Innovation at Brookings will host experts for a half-day forum on the development of this framework and privacy risk management. Through keynotes and panel discussions, experts will share their perspectives on the current and future state of privacy practices from both an implementation and policy perspective, as well as the potential domestic and international impact of this privacy framework. Attendees will learn directly from NIST leadership about their plans for the framework development, hear industry responses, and explore the issues presented by a framework approach to privacy.

After each panel, speakers will take audience questions. You can also follow the conversation on Twitter using **#PrivacyFramework**.

9:00 am Opening remarks

Cameron Kerry, Ann R. and Andrew H. Tisch Distinguished Visiting Fellow, Governance Studies, The Brookings Institution

9:05 am The NIST Privacy Framework: The road ahead

Walter Copan, Director, National Institute of Standards and Technology, U.S. Department of Commerce

9:25 am Industry principles for privacy risk management

Dean C. Garfield, President and CEO, Information Technology Industry Council

9:45 am What does risk management mean in the context of privacy?

Moderator: Cameron Kerry, Ann R. and Andrew H. Tisch Distinguished Visiting Fellow, Governance Studies, The Brookings Institution
Harriet Pearson, Partner, Hogan Lovells US LLP
David Hoffman, Director of Security Policy and Global Privacy Officer, Intel Corporation
Travis Hall, Telecommunications Policy Analyst, National Telecommunications and Information Administration, U.S. Department of Commerce
Michelle Richardson, Director of the Privacy and Data Project, Center for Democracy and Technology

10:45 am Break

10:55 am What are the practices and tools that can inform a privacy framework?

Moderator: Naomi Lefkovitz, Senior Privacy Policy Advisor, National Institute of Standards and Technology, U.S. Department of Commerce
Jenn Behrens, Partner and Executive Vice President of Privacy, KUMA LLC
Kevin Gay, Chief of Intelligent Transportation Systems Policy, Architecture, and Knowledge Transfer, Federal Highway Administration, U.S. Department of Transportation
Harley Geiger, Director of Public Policy, Rapid7
Zoe Strickland, Managing Director and Global Chief Privacy Officer, JP Morgan Chase
John Verdi, Vice President of Policy, Future of Privacy Forum

11:55 am Closing remarks

Cameron Kerry, Ann R. and Andrew H. Tisch Distinguished Visiting Fellow, Governance Studies, The Brookings Institution

Opening remarks

Cameron Kerry

Cameron Kerry joined Governance Studies and the Center for Technology Innovation at Brookings as the first Ann R. and Andrew H. Tisch distinguished visiting fellow in December 2013. In addition to his Brookings affiliation, Cameron Kerry is senior counsel at Sidley Austin, LLP in Boston and Washington, D.C., and a visiting scholar the MIT Media Lab. His practice at Sidley Austin involves privacy, security, and international trade issues.

Kerry served as general counsel and acting secretary of the United States Department of Commerce, where he was a leader on a wide of range of issues laying a new foundation for U.S. economic growth in a global marketplace. He continues to speak and write on these issues, particularly privacy and data security, intellectual property, and international trade.

While acting secretary, Kerry served as chief executive of this Cabinet agency and its 43,000 employees around the world, as well as an adviser to the President. His tenure marked the first time in U.S. history two siblings have served in the President's Cabinet at the same time.

As general counsel, he was the principal legal adviser to the several Secretaries of Commerce and Commerce agency heads, and oversaw the work of more than 400 lawyers across these agencies. He was a leader in the Obama administration's successful effort to pass the America Invents Act, the most significant overhaul of the patent system in more 150 years. As co-chair of the National Science & Technology Council Subcommittee on Privacy and Internet Policy, he spearheaded development of the White House blueprint on consumer privacy, Consumer Data Privacy in a Networked World. He then led the administration's implementation of the blueprint, drafting privacy legislation and engaging on privacy issues with international partners, including the European Union. He helped establish and lead the Commerce Department's Internet Policy Task Force, which brings together agencies with expertise in the 21st Century digital economy.

He also played a significant role on intellectual property policy and litigation, cybersecurity, international bribery, trade relations and rule of law development in China, the Gulf oil spill litigation, and many other challenges facing a large, diverse federal agency. He travelled to the People's Republic of China on numerous occasions to co-lead the transparency dialogue with China as well as the U.S. / China Legal Exchange and exchanges on anti-corruption.

Before his appointment to the Obama administration in 2009, Kerry practiced law at the Mintz Levin firm in Boston and Washington. His practice covered a range of complex commercial litigation and regulation of telecommunications. He tried cases involving significant environmental and scientific evidence issues and taught telecommunications law as an adjunct professor at Suffolk University Law School.

Prior to joining Mintz Levin, he was an associate at Wilmer Cutler & Pickering in Washington, D.C. and a law clerk to Senior Circuit Judge Elbert P. Tuttle of the United States Court of Appeals for the Fifth Circuit. During the 2004 presidential campaign, Kerry was a close adviser and national surrogate for democratic nominee John Kerry. He has been deeply involved in electoral politics throughout his adult life. He is a magna cum laude graduate of Boston College Law School (1978), where he was winner of the school's moot court competition and a law review editor, and a cum laude graduate of Harvard College (1972).

Cameron Kerry also has been actively engaged in politics and community service throughout his adult life. In 2004-04, he was a senior adviser and national surrogate in the U.S. presidential campaign, traveling to 29 states and Israel. He has served on the boards of non-profits involved in civic engagement and sports.

The Ann R. and Andrew H. Tisch distinguished visiting fellows in Governance Studies are individuals of particularly noteworthy distinction. The fellowship is designed to bring distinguished visitors from government, business, journalism, and academia to Brookings to write about challenges facing the country. Kerry is the first to be named to this prestigious fellowship.

Keynotes

Walter G. Copan

Walter G. Copan was confirmed by Congress as undersecretary of commerce for standards and technology and NIST director on October 5, 2017. As NIST director, Copan provides high-level oversight and direction for NIST. He has had a distinguished and diverse career as a science and technology executive in large and small corporations, U.S. government, nonprofit and other public-sector settings.

Copan formerly served as president and CEO of the IP Engineering Group Corporation, providing services in intellectual property strategy, technology commercialization and innovation. Until June 2017, he was founding CEO and chairman of Impact Engineered Wood Corporation, an advanced materials technology company. He also is a founding board member of Rocky Mountain Innovation Partners, where he led technology transfer programs and innovation services on behalf of the U.S. Air Force Academy, U.S. federal labs and academic institutions and helped foster entrepreneurial businesses in the Rocky Mountain West. He also served with the National Advisory Council to the Federal Laboratory Consortium for more than five years, providing industry inputs to advance the U.S. economic impacts of the federal laboratory system.

From 2010–2013, Copan served as managing director of Technology Commercialization and Partnerships at DOE's Brookhaven National Laboratory (BNL). Among his accomplishments were leading the creation and implementation of the new DOE technology transfer mechanism, Agreement for Commercializing Technology (ACT), to facilitate collaborations between the federal labs and U.S. corporations. He led the Startup America initiative on behalf of DOE for entrepreneurial business creation, and he initiated the DOE's new Small Business Innovation Research – Technology Transfer (SBIR-TT) program, which built upon the experiences of NIST. He served as founding partner and board member of the Accelerate Long Island alliance for innovation, economic development and early stage investment.

From 2005–2010, Copan was executive vice president and chief technology officer at Clean Diesel Technologies, Inc., an international technology development and licensing firm. He spearheaded the company's transformation, growth and listing on NASDAQ (CDTI), as well as the company's subsequent merger. Prior to joining CDTI, Copan served at the DOE's National Renewable Energy Laboratory (NREL) as Principal Licensing Executive, Technology Transfer. There, he led organizational changes that strengthened relationships with industry and the investment community, and led to the more productive commercialization of energy-related technologies.

After earning dual B.S. and B.A. degrees in chemistry and music from Case Western Reserve University in

1975, Copan began his career in chemicals and materials research at the Lubrizol Corporation (now part of the Berkshire Hathaway Group). He earned a Ph.D. in physical chemistry from Case Western in 1982, and subsequently held leadership positions at Lubrizol in research and development, strategy, business unit management, venture capital, and mergers, acquisitions and strategic alliances in the U.S. and abroad. As managing director,

Technology Transfer and Licensing, from 1999–2003, he was responsible for Lubrizol's corporate venturing and open innovation, technology strategy, business development, intellectual assets and the technology licensing business.

Copan is a patent holder, has authored numerous professional publications and presentations, and has served on the boards of many organizations; including the Licensing Executives Society (LES) USA and Canada, where he recently served as regional vice president for LES USA. He has contributed to the U.S. National Academy of Sciences, the Council on Competitiveness, the World Intellectual Property Organization and the United Nations on innovation, technology transfer, energy and economic development matters.

Dean Garfield

Dean Garfield is the president and CEO of ITI. Since taking on this role in 2009, Dean has built ITI into the global voice of the tech sector and membership has nearly doubled. He leads a team of professionals who, combined, bring nearly three centuries of advocacy experience to bear on the most complex policy challenges facing the world's leading and most innovative technology companies.

Garfield has worked to foster a policy environment that embraces cutting-edge research, game-changing technologies, and national economic champions as central to the foundation for sustained job creation and growth. The results: the tech sector has continued to grow despite global economic challenges. Companies are expanding — putting more people to work, creating breakthrough products and services, and expanding into new markets with enormous opportunity. Under Dean's leadership, ITI has defined the tech agenda for global policymakers, expanded its membership and influence, and launched a foundation that serves as the preeminent thought leader on innovation. ITI has deepened its expertise on core issues — from trade and new market development to taxes, from cloud computing to core standards. During Garfield's tenure, ITI's advocacy experts have helped to achieve critical legislative victories in the U.S. and internationally, knocking down barriers to innovation, strengthening America's economic competitiveness, and advancing sustainable technologies that will be at the heart of 21st century innovation.

Prior to joining ITI, Dean served as executive vice president and chief strategic officer for the Motion Picture Association of America (MPAA). While there, he developed the association's global strategies, securing accomplishment of key operational objectives, forged industry alliances on behalf of the MPAA, and led the MPAA's research and technology departments. Dean also represented the MPAA before legislative bodies and at key conferences around the world, including the European Commission and Oxford University.

Dean also served as vice president of legal affairs at the Recording Industry Association of America (RIAA). He helped to develop the organization's comprehensive intellectual property policy and litigation strategies and managed several of the United States' most important intellectual property cases, including the Grokster/Kazaa case, from its filing to its resolution at the Supreme Court.

He received a joint degree from New York University School of Law and the Woodrow Wilson School of Public Administration and International Affairs at Princeton University. He was a Ford-Rockefeller as well as a Root-Tilden-Snow scholar.

Panel 1

Travis Hall

Travis Hall is a telecommunications policy specialist for the National Telecommunications and Information Administration's Office of Policy and Development, focusing on surveillance and consumer privacy.

His portfolio includes IoT, UAS, and Blockchain, and he recently successfully concluded two privacy multistakeholder processes. He has a Ph.D. from the Department of Media, Culture and Communication from New York University, and his dissertation research focused on the cultural contexts and histories of state identification programs, specifically those that use bodies as the media of identity (biometrics, tattoos). He has acted as a consultant for advocacy groups, academic institutes, and private companies on the technical and policy details of identification and the potential impacts of these technologies on privacy rights. Before joining the Department of Commerce, Hall taught at American University and was a research fellow at the Humboldt Institute for Internet and Society in Berlin, Germany. He received his M.A. in international communications and B.A. in international relations from American University.

Daniel A. Hoffman

David A. Hoffman is associate general counsel and global privacy officer at Intel Corporation, in which capacity he heads the organization that oversees Intel's privacy compliance activities, legal support for privacy and security, and all external privacy/security engagements.

Hoffman joined Intel in 1998 as Intel's eBusiness attorney to manage the team providing legal support for Intel's chief information officer. In 2005, Mr. Hoffman moved to Munich, Germany, as group counsel in the Intel European Legal Department, while leading Intel's Worldwide Privacy and Security Policy Team.

Hoffman served on the TRUSTe Board of Directors from 2000-2006. From 2005 – 2009, Hoffman served on the Board of Directors for the International Association of Privacy Professionals, and he is currently a member of the Advisory Board for the Future of Privacy Forum and the Board of the Information Accountability Foundation. He also chairs the board for the Coalition for Cybersecurity Policy and Law. Hoffman is a senior lecturing fellow at the Duke University School of Law.

Hoffman has a J.D. from The Duke University School of Law, where he was a member of the Duke Law Review. Hoffman also received an A.B. with honors from Hamilton College.

Peter Lefkowitz

Peter Lefkowitz is chief privacy & digital risk officer at Citrix Systems. Peter oversees legal and regulatory risk associated with data, products and systems, as well as policy engagement on digital issues.

Prior to joining Citrix, Lefkowitz worked at GE, where he served as chief privacy officer (corporate) and then as senior data rights management counsel (digital) and at Oracle, where he was vice president of privacy and security legal and chief privacy officer. Lefkowitz is Chairman of the Board of the International Association of Privacy Professionals and a member of the Boston Bar Association Council. Lefkowitz holds a Bachelor of Arts in history, magna cum laude, from Yale College and a law degree from Harvard Law School.

Harriet Pearson

Harriet Pearson currently leads Hogan Lovells' global multidisciplinary cybersecurity practice and serves as the firm's first innovation and new ventures partner, a role in which she is responsible for sparking and supporting ideas for new client solutions.

Internationally recognized as a corporate data privacy and cybersecurity pioneer, Pearson brings to her practice decades of leading-edge experience advising companies and boards on cyber and data risk management and governance, breach preparedness and response, crisis management, global data privacy compliance, and public policy strategies.

The Financial Times recognized Harriet in 2016 as North America Legal Innovator of the Year. Lawdragon named her as one of the 500 Leading Lawyers in America from 2015 to 2018, and the National Law Journal recognized her in 2015 as a Cybersecurity and Privacy Trailblazer. Clients seek out Harriet's unique mix of legal, compliance, and business skills. Harriet joined Hogan Lovells in 2012 from the IBM Corporation, where among other roles she served as vice president security counsel and chief privacy officer (CPO) from 2000-12.

Harriet co-founded and has co-chaired the Georgetown Cybersecurity Law Institute since 2012 and serves on a number of advisory boards. She helped found and served for a decade on the board of the International Association of Privacy Professionals, an organization that recognized her longstanding leadership in the privacy field in 2007 by awarding her its Vanguard Award.

Michelle Richardson

Michelle Richardson is the director of the data and privacy project where she leads CDT's efforts to create a user-centered internet. Her team engages companies and government officials to create policies and technical solutions that protect individual privacy, empower users, and advance social justice.

Michelle has testified before Congress, advised government agencies, and frequently appears in national press such as The Washington Post, The New York Times, NPR, and Politico. Recognized by The Hill as one of the most influential nonprofits lobbyists in Washington, she has led left-right coalitions to defend privacy in the face of ever-expanding government authorities.

Before joining CDT in 2017, Michelle led the American Civil Liberties Union's preeminent legislative campaigns against overreaching surveillance programs for 10 years. She also served as a democratic counsel for the House Judiciary Committee where she worked on a range of anti-terrorism laws and policies. She received her B.A. from the University of Colorado and her J.D. from American University, Washington College of Law. She currently serves as a senior fellow at George Washington University's Center for Cyber and Homeland Security.

Panel 2

Jenn Behrens

Jenn Behrens is partner and executive vice president of Kuma. She specializes in privacy, governance, and identity management and leads our privacy service offering. Behrens focuses on supporting organizations in transition from compliance to commitment in privacy excellence in identity management.

She has vast experience in leading privacy related efforts for multiple federal (NSTIC) pilots as well as in providing privacy gap assessment and risk mitigation methodologies in conjunction with developing compliance strategies for both government and industry organizations.

Behrens is the IDESG plenary chair (former privacy committee chair), is an IAPP Women Leading Privacy Advisory Board Member, and is a HIMSS Patient Identity Integrity Workgroup member. Jenn received her B.A. from UVA, M.S.W. from VCU, and Ph.D. in public policy and administration from VCU. Jennifer holds CIPP/US, CIPP/G, CIPM and CHPSE credentials.

Kevin Gay

Gay is the chief of the ITS Policy group in the Intelligent Transportation Systems Joint Program Office at the U.S. Department of Transportation. Gay leads a group program managers responsible for executing a portion of the $100M ITS annual research portfolio to support the development and deployment of ITS technology. Gay's group includes both enabling technology and policy research in the areas of radio frequency spectrum, cybersecurity, standards, architecture, data management and privacy.

Gay previously worked for the National Highway Traffic Safety Administration (NHTSA) as the program manager for the development of the Connected Vehicle Security Credential Management System (SCMS), which developed a proof-of-concept system to demonstrate feasibility for trusted vehicle-to-vehicle and vehicle-to-infrastructure communications.

Prior to that, Gay led a team of researchers at the Volpe National Transportation Systems Center in the development of the 5-year program plan for vehicle automation research at the U.S. DOT. Prior to this, Gay managed the technical day-to-day aspects of the Connected Vehicle Safety Pilot Model Deployment in Ann Arbor, Michigan, which was a yearlong field operational test of dedicated short-range communications (DSRC) based crash avoidance systems involving thousands of motor vehicles and corresponding roadside systems.

Gay is certified as a project management professional (PMP) and has a Bachelor of Science in applied mathematics from the Georgia Institute of Technology.

Harley Geiger

Harley Geiger is director of public policy at Rapid7, where he leads the company's policy engagement and government affairs activities on cybersecurity, privacy, computer crime, exports, and digital trade issues.

Prior to working at Rapid7, Geiger was advocacy director at the Center for Democracy & Technology (CDT), where he worked on issues related to government surveillance, privacy, and computer crime. Prior to that, Geiger was senior legislative counsel for U.S. Representative Zoe Lofgren of California, serving as lead staffer for technology and intellectual property issues. Geiger is an attorney and is CIPP/US certified.

Naomi Lefkovitz

Naomi Lefkovitz is the senior privacy policy advisor in the Information Technology Lab at the National Institute of Standards and Technology, U.S. Department of Commerce. She leads the privacy engineering program, which focuses on developing privacy risk management processes

and integrating solutions for protecting individuals' privacy into information technologies, including digital identity services, IoT, smart cities, big data, mobile, and artificial intelligence.

FierceGovernmentIT named Ms. Lefkovitz on their 2013 "Fierce15" list of the most forward-thinking people working within government information technology, and she is a 2014 and 2018 Federal 100 Awards winner.

Before joining NIST, she was the director for privacy and civil liberties in the Cybersecurity Directorate of the National Security Council in the Executive Office of the President. Her portfolio included the National Strategy for Trusted Identities in Cyberspace as well as addressing the privacy and civil liberties impact of the Obama administration's cybersecurity initiatives and programs.

Prior to her tenure in the Obama administration, Lefkovitz was a senior attorney with the Division of Privacy and Identity Protection at the Federal Trade Commission. Her responsibilities focused primarily on policy matters, including legislation, rulemakings, and business and consumer education in the areas of identity theft, data security and privacy. At the outset of her career, she was assistant general counsel at CDnow, Inc., an early online music retailer.

Lefkovitz holds a B.A. with honors in French literature from Bryn Mawr College and a J.D. with honors from Temple University School of Law.

Zoe Strickland

Zoe Strickland is the managing director, global chief privacy officer, for JPMorgan Chase. She is responsible for domestic and global privacy compliance at the company enterprise level, including its privacy policies, procedures, governance, strategy, training, and administration.

Previously, Strickland served as the VP chief privacy officer for UnitedHealth Group and for Walmart Stores Inc. Strickland is an active participant in the privacy community. She serves on the Advisory Board of the Future of Privacy Forum and several other cross-industry organizations. She previously served on the Board of Directors for the International Association of Privacy Professionals (IAPP). Strickland is a frequent speaker at industry conferences and events, has testified before subcommittees of the House Energy and Commerce Committee, and has been quoted in national and trade media sources, including USA Today, the New York Times, and National Public Radio.

John Verdi

John Verdi is vice president of policy at the Future of Privacy Forum (FPF). John supervises FPF's policy portfolio, which advances FPF's agenda on a broad range of issues, including artificial intelligence & machine learning, algorithmic decision-making, ethics, connected cars, smart communities, student privacy, health, the internet of things, wearable technologies, de-identification, and drones.

Verdi previously served as director of privacy initiatives at the National Telecommunications and Information Administration, where he crafted policy recommendations for the U.S. Department of Commerce and President Obama regarding technology, trust, and innovation. John led NTIA's privacy multi-stakeholder process, which established best practices regarding unmanned aircraft systems, facial recognition technology, and mobile apps. Prior to NTIA, he was general counsel for the Electronic Privacy Information Center (EPIC), where he oversaw EPIC's litigation program. John earned his J.D. from Harvard Law School and his B.A. in philosophy, politics, and law from SUNY-Binghamton.

BROOKINGS

Add to Brookings Mailing Lists

To be added to various Brookings mailing lists, please complete the information below.

Name: _____ Email: _____

Organization: _____ Title: _____

City/State/Zip: _____

☐ **I would like to receive the Governance Studies Update, a weekly newsletter on governance issues and the political process from Governance Studies at Brookings.**

Other newsletters that might interest you are:

☐ Events Update, a weekly digest of upcoming events hosted by Brookings in Washington, D.C.
☐ Brookings Brief, a frequent email with updates from Brookings experts on top issues of the day.

I would also like to be invited to events on the following topics:

☐ Africa
☐ Arms Control
☐ Asia Economy
☐ Banking Finance
☐ BRICS
☐ Budget
☐ Campaign Finance
☐ Children and Families
☐ China
☐ Civil Liberties
☐ Climate Change
☐ Democracy Promotion
☐ Demographics
☐ Economy
☐ Education
☐ Elections
☐ Energy
☐ Europe
☐ Foreign Aid
☐ Global Cities
☐ Global Health
☐ Global Poverty
☐ Government
☐ Health Care
☐ Higher Education
☐ Homeland Security
☐ IMF/World Bank/G20
☐ Immigration
☐ India
☐ Infrastructure
☐ Japan
☐ Justice and Law
☐ Korea
☐ Labor
☐ Latin America
☐ Metropolitan Policy
☐ Middle East
☐ Middle East Economics
☐ Military and Defense
☐ Politics
☐ Race
☐ Religion
☐ Russia
☐ Social Mobility
☐ South America
☐ Taxes
☐ Technology
☐ Terrorism
☐ Trade
☐ Transportation
☐ Turkey
☐ United Nations
☐ U.S. Congress
☐ U.S. Poverty
☐ Women's Issues

Californians have new privacy protections. Google wants Republicans to weaken them.

BY EMILY CADEI
ecadei@mcclatchydc.com

WASHINGTON
Two weeks ago, the nation's tech titans came to Washington to urge Congress to pass legislation that would override the data privacy law California's legislature passed in June. On Wednesday, privacy advocates got their chance to push back.

"We understand this committee is considering a national standard for data privacy, but we implore you not to weaken or undo the safeguards (the new California law) has so recently put in place, which now cover 40 million Americans," said Alastair Mactaggart, the wealthy Northern California real estate developer who spearheaded the campaign to enact the California Consumer Privacy Act.

Other like-minded academics and policymakers echoed Mactaggart's pleas to senators on the Commerce, Science and Transportation Committee.

"Existing privacy protections should not be weakened," said Nuala O'Connor, president and CEO of the Center for Democracy and Technology, a nonprofit that advocates for online civil liberties. Any new federal law "should include individual rights like the ability to access, correct and delete personal information," O'Connor added, values that "are already ensconced both in the California law and the GDPR," a European Union data privacy law that went into effect this past spring.

Their testimony underscores how much California's law, which does not go into effect until 2020, figures into the national furor over Americans' right to privacy in the digital age, sparked by Facebook's Cambridge Analytica scandal and other massive breaches of users' online information that have come to light in recent months. They also highlight how much the state measure could be undermined by ongoing lobbying effort to modify it, via federal action as well as in the state Legislature.

Representatives for Google, Twitter, Apple, Amazon, AT&T and Charter Communications argued before the same Senate committee on Sept. 26 that Congress needed to pass a federal data standard to prevent a "patchwork" of state laws, like California's.

"Providers struggling with compliance may have no choice but to adopt the most restrictive elements of each state's law, given the impracticability of complying with multiple state rules," warned Leonard Cali, senior vice president of global public policy at AT&T. "The result may be a more restrictive privacy framework than any state intended with less innovation,investment and consumer welfare."

Cali called for a new federal law that "learns from" and "does better than" the California Consumer Privacy Act and the European Union law. Fellow executives reiterated that imperative.

In his opening statement, Mactaggart pooh-poohed the companies' criticism as alarmist.

"You heard from representatives of giant corporations only two weeks ago that the sky will essentially fall if you leave (California's law) intact," he said. "This law was rushed and badly drafted, they said, and it needs preemption right away."

"On the contrary," Mactaggart continued, "we spent years talking to legal and technical experts, academics, businesses, privacy advocates. And its language reflects thousands of hours of careful drafting."

California policymakers reached a hasty agreement on the data privacy law in the face of a Mactaggart-funded ballot initiative campaign to put an even more stringent law before the voters in November. Mactaggart agreed to pull the ballot measure when the Legislature passed the compromise bill on June 28. Some privacy advocates feared the legislation did not go far enough. Californian companies from a range of industries, meanwhile, have continued to press for "corrections" to the law that would tighten definitions and prevent what they argue is overreach.

Senators on Wednesday raised some of those same issues with the privacy advocates, suggesting a sympathy with the Internet industry and other critics of the law. Republican lawmakers appeared particularly skeptical, hinting at a partisan divide that was absent from the California Legislature.

"Are you concerned that that broad definition of personal information sweeps in information that isn't sensitive?" Kansas Republican Jerry Moran asked Mactaggart. The language in the California law "sounds somewhat removed from information that can identify an individual," Moran added.

Republican Roger Wicker of Mississippi, meanwhile probed the witnesses about how a patchwork of state privacy laws would “affect consumers adversely.”