This space is for the Federal Privacy Council. Users will only see collaborations to which they have specifically been given access by the collaboration owner.

PERMISSIONS _ OPEN-EXECUTIVE BRANCH

Pages / Home / Federal Privacy Council Home Page

FEDERAL PRIVACY SUMMIT 2021

Created by Sari Wilson (GSA), last modified on Nov 03, 2021

PRIVACY COUNCIL

Search

Council Home Full Council Committees Training and Resources FPC.gov

SUMMIT INFORMATION

DATE: Wednesday, November 3, 2021

TIME: All day

LOCATION: Virtual (ZoomGov). Registrants will receive zoom information via email prior to the event.

SUMMIT MATERIALS:

2021 FEDERAL PRIVACY SUMMIT - **PROGRAM GUIDE**

2021 FEDERAL PRIVACY SUMMIT - **OVERVIEW SLIDE DECK**

2021 FEDERAL PRIVACY SUMMIT - BREAKOUT SESSION SLIDE DECKS

- **Privacy Case Law Update 2021**
- **CNSS and Privacy**
- **Decentralized Identifiers: How DIDs Can Help Reduce the Use of SSNs as Authenticators**
- NIST SP 800-53A, Revision 5: Latest Updates and Tools for Conducting Effective Control Assessments
- Privacy Risks, Civil Liberties Risks, and Publicly Available Data (no slides)
- **Negotiating Data Sharing Agreements: Case Studies, Trip-ups, and Tools**
- **The Responsible Collection of Diversity, Equity, and Inclusion Data**
- **Identify and Remediate Instances of PII in Free Text**
- **Cross-Border Data Flows and Government Access to Data: Commercial and National Security Perspectives**

2021 FEDERAL PRIVACY SUMMIT OVERVIEW

The Federal Privacy Summit draws privacy professionals from across the Executive Branch. In addition to featuring exciting speakers and topics, this event includes the presentation of FPC Awards, which recognize the extraordinary achievements of Federal privacy professionals. It is free of charge and open to Federal employees and contractors in the Executive Branch.

No labels

CHILD PAGES (1)

xx

ATTACHMENTS (10)

2021 FPC Summit Slides - FINAL.pptx
Last edited by: Sari Wilson (GSA) on Nov 03, 2021 at 07:34 AM
No labels

Responsible Collection of DEIA Data (1) (1).pptx
Last edited by: Sari Wilson (GSA) on Nov 02, 2021 at 12:45 PM
No labels

DIDs Panel FPC Summit-Final.pptx
Last edited by: Sari Wilson (GSA) on Nov 02, 2021 at 12:45 PM
No labels

Privacy Case Law Update.pptx
Last edited by: Sari Wilson (GSA) on Nov 02, 2021 at 12:44 PM
No labels

2021 Federal Privacy Summit Program Book (1).pdf
Last edited by: Sari Wilson (GSA) on Nov 02, 2021 at 12:34 PM
No labels

Negotiating Data Sharing Agreements_ Case Studies, Trip-ups, and Tools.pptx
Last edited by: Sari Wilson (GSA) on Oct 29, 2021 at 03:30 PM
No labels

Identify and Remediate Instances of PII in Free Text _ Master.pptx
Last edited by: Sari Wilson (GSA) on Oct 29, 2021 at 03:29 PM
No labels

Cross-Border Data Flows and Government Access to Data_.pptx
Last edited by: Sari Wilson (GSA) on Oct 29, 2021 at 03:29 PM
No labels

CNSS and Privacy FPC Summit 20211026.pptx
Last edited by: Sari Wilson (GSA) on Oct 29, 2021 at 03:28 PM
No labels

fpc_logo.png
Last edited by: Christian Sierra (GSA,Ctr) on Oct 14, 2021 at 10:35 AM
No labels

COMMENTS(2)

Kimberly Burch (FMSHRC) Posted Oct 18, 2021 at 03:56 PM

Can you register for this event and only participate in some of the sessions?

Reply Hide

Catherine England (COE) Posted Nov 03, 2021 at 02:19 PM

Can you republish the NIST slides? The link above (Summit Information) is not correct and the slides are not showing up in Attachments tab. Thank you.

Reply Hide

2021 FEDERAL PRIVACY SUMMIT AGENDA

November 3, 2021

9:00am - 9:15am	Welcome and Logistics	Shenaye Holmes, FPC Senior Advisor, GSA
9:15am - 9:45am	Opening Remarks and FPC awards	Kirsten Moncada, FPC Chair and OIRA Privacy Branch Chief, OMB
9:45am-10:45am	BREAKOUT 1 (choose one)	
	Privacy Case Law Update 2021	***Speakers:*** (b) (7)(C) [redacted]
	CNSS and Privacy	***Moderator:*** Rebecca Richards, NSA ***Speakers:*** AndraLeigh (Andy) Rodini, DOE (b) (7)(C) [redacted]
	Decentralized Identifiers: How DIDs Can Help Reduce the Use of SSNs as an Authenticator	***Moderator:*** Charlie Cutshall, CFTC ***Speakers:*** (b) (7)(C) [redacted] Naomi Lefkovitz, NIST
10:45am -11:00am	BREAK	
11:00 am-12:30 pm	**Keynote Panel: Privacy and Equity** While protecting privacy in our increasingly connected society is no easy task, doing so is more than just an administrative nicety. Instead, as the keynote panel will discuss, privacy is a critical first order right that helps ensure the safety, civil rights, economic stability, and enfranchisement of marginalized communities, while also advancing critical democratic values. In the same way that surveillance can be used to control individuals, privacy can empower them to craft their own identities, resist violence, and shape the public sphere. As a result, whether government agencies are deploying data-centric technologies or regulating them, agencies need to consider the perspectives and privacy needs of marginalized people. ***Panelists:*** Khiara M. Bridges, Professor of Law, UC Berkeley School of Law Scott Skinner-Thompson, Associate Professor, University of Colorado Law School Michele Gilman, Professor of Law, University of Baltimore School of Law	

	Moderators: Kirsten Moncada, FPC Chair (OMB) Joo Chung, FPC Vice-Chair (DOD)	
12:30pm -1:30pm	BREAK	
1:30pm - 2:30pm	BREAKOUT 2 (choose one)	
	NIST SP 800-53A, Revision 5: Latest Updates and Tools for Conducting Effective Control Assessments	***Speakers:*** Alaina Nguyen, PBGC Claire Barrett, NIST Victoria Yan Pillitteri, NIST
	Privacy Risks, Civil Liberties Risks, and Publicly Available Data	***Moderator:*** Rebecca Richards, NSA ***Speakers:*** (b) (7)(C) [redacted]
	Negotiating Data Sharing Agreements: Case Studies, Trip-ups, and Tools	***Speakers:*** (b) (7)(C) [redacted] Maya Bernstein, HHS Megan Metcalf, USAID Todd Anderson, USAID
2:30pm - 2:45pm	BREAK	
2:45pm -3:45pm	BREAKOUT 3 (choose one)	
	The Responsible Collection of Diversity, Equity, and Inclusion Data	***Speakers:*** Suzanne Wachter, USAID Jessica Holzberg, U.S. Census Bureau Darrell Overbey, EEOC Agnes O'Hanlon, USAID
	Identify and Remediate Instances of PII in Free Text	***Moderator:*** Donna Miller, CDC ***Speakers:*** Chad Tompkins, CFPB Travis Hoppe, CDC William Frankenstein, State
	Cross-Border Data Flows and Government Access to Data: Commercial and National Security Perspectives	***Moderator***: Nasreen Djouini, ITA ***Speakers:*** Clinton Harper, ITA (b) (6) [redacted] Sam Schofield, ITA

2021 FEDERAL PRIVACY SUMMIT

November 3, 2021

Federal Privacy Council

Navigating the Summit

Refer to the 2021 Privacy Summit Program Book for:

- Summit Overview & Schedule
- Keynote Panel & Breakout Session Overviews
- FAQs & Tech Support Tips

Schedule at a Glance

9:00am - 9:15am	**Welcome and Logistics**
9:15am - 9:45am	**Opening Remarks and FPC awards**
9:45am - 10:45am	**Breakout Session 1**
10:45am - 11:00am	**Break**
11:00am - 12:30pm	**Keynote Panel: Privacy and Equity**
12:30pm - 1:30pm	**Lunch Break**
1:30pm - 2:30pm	**Breakout Session 2**
2:30pm - 2:45pm	**Break**
2:45pm - 3:45pm	**Closing Remarks & Breakout Session 3**

Housekeeping

- Attendance, Participation and Engagement through Zoom
- Visit the OMB MAX Page to access the Privacy Summit slide decks, program book, and other materials.
- CIPP, CIPM, and CIPT holders are eligible to receive 1 IAPP CPE credit per event hour.

Housekeeping

- This event is not recorded and is not open to the press.
- Due to the size of the event, attendees will not have the ability to unmute or turn on their video, unless prompted by a moderator.
- Attendees are encouraged to participate through enabled chat options during the breakout sessions.

FPC Reflections:
Looking Back & Moving Forward

Get Involved in 2022!

Working Groups

Communities of Practice

Cross-Council Engagement

Community Outreach

Sharing Best Practices

2021 FPC Awards for Excellence

Department of Defense (DoD) Privacy Training Team

Maya A. Bernstein

Health and Human Services

Breakout Room Logistics

Self Select the Zoom Breakout Room of your choice

Session 1

9:45 am - 10:45 am

Breakout Options:

- Privacy Case Law Update 2021
- CNSS and Privacy
- Decentralized Identifiers: How DIDs Can Help Reduce the Use of SSNs as an Authenticator

Break

10:45 am - 11:00 am

Keynote Panel: Privacy & Equity

Khiara M. Bridges
Professor of Law
UC Berkeley School of Law

Scott Skinner-Thompson
Associate Professor
University of Colorado Law School

Michele Gilman
Professor of Law & Associate Dean
University of Baltimore School of Law

Break

12:30 pm - 1:30 pm

Session 2

1:30pm – 2:30pm

Breakout Options:

NIST SP 800-53A, Revision 5: Latest Updates and Tools for Conducting Effective Control Assessments

Privacy Risks, Civil Liberties Risks, and Publicly Available Data

Negotiating Data Sharing Agreements: Case Studies, Trip-ups, and Tools

Break

2:30 pm - 2:45 pm

Session 3

2:45pm – 3:45pm

Breakout Options:

- The Responsible Collection of Diversity, Equity and Inclusion Data
- Identify and Remediate Instances of PII in Free Text
- Cross-Border Data Flows and Government Access to Data: Commercial and National Security Perspectives

Thank you for participating in the 2021 Federal Privacy Summit!

Responsible Collection of Diversity, Equity, Inclusion and Accessibility Data

Federal Privacy Summit

U.S. Agency for International Development
U.S. Census Bureau
Equal Employment Opportunity Commission

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

- The information provided in this slide deck is for informational purposes only and should not be understood as legal advice.
- This presentation is only for US Government Distribution.
- The opinions expressed are personal opinions of the speakers, and not of their respective agencies.

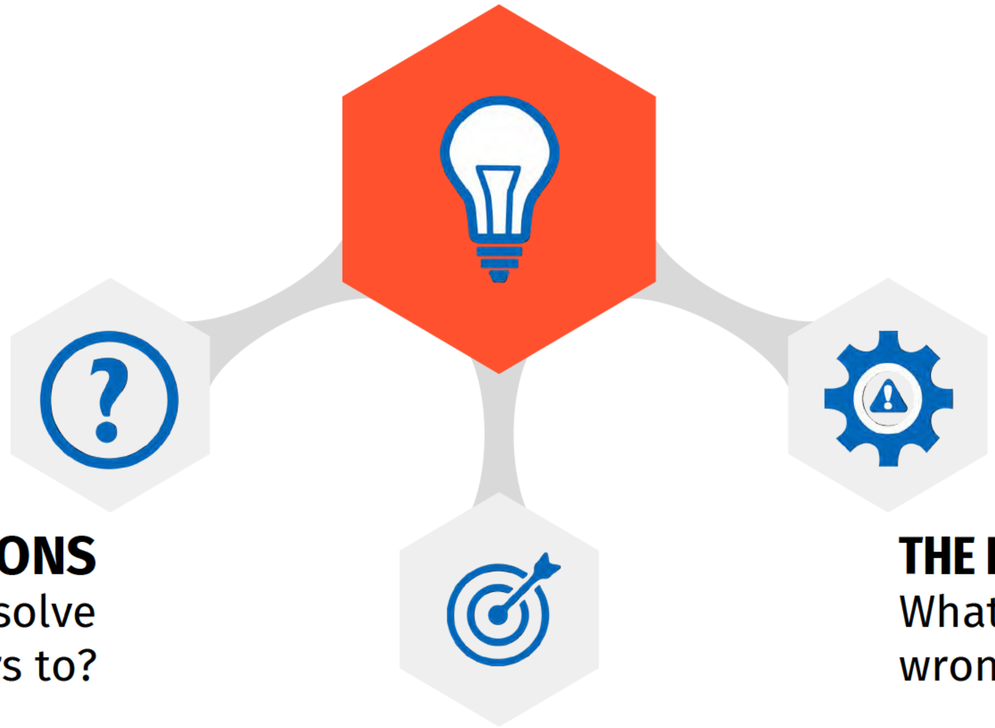
US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

The Rules

01	Executive Orders	• Executive Order 14035 • Executive Order 13985
02	OMB Circular A-130, Definition of PII	• Linked or linkable • The Mosaic Effect
03	Privacy Act Statements and Notices	• Reassurance • Increase Participation
04	Paperwork Reduction Act	• Depends on participants
05	Title VII, Civil Rights Act and the Rehabilitation Act	• Employee protection and rights

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

Pre-Collection Considerations



THE QUESTIONS
What are we trying to solve or find answers to?

THE PURPOSE
What's the goal of the collection?

THE RISK
What's the risk of getting it wrong?

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

Post Collection Considerations

01	ETHICS
02	RISKS OF RE-IDENTIFICATION
03	CONTINUED USE OF THE DATA
04	TRANSPARENCY

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

Questions

Panel

Suzanne Wachter, USAID, swachter@usaid.gov

Jessica Holzberg, Census, jessica.holzberg@census.gov

Darrell Overbey, EEOC, darrell.overbey@eeoc.gov

Agnes O'Hanlon, USAID, aohanlon@usaid.gov

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

Decentralized Identifiers

How Decentralized Identifiers Can Help Reduce the Use of Social Security Numbers as an Authenticator

(b) (7)(C) [redacted]
(b) (7)(C) [redacted]

(b) (7)(C) [redacted]
(b) (7)(C) [redacted]
[redacted]

Naomi Lefkovitz

Senior Privacy Policy Advisor, NIST

Charles Cutshall

Chief Privacy Officer, Legal Division, CFTC

SSN and Identity Theft in the US

- The SSN's effectiveness as an identifier – a unique number that enables individuals to be associated with information – has contributed to its widespread use

- Using the SSN as an authenticator – something individuals possess and control such as a cryptographic module or password to verify their identities – has contributed to identity theft

Security in Numbers

*** - ** - ****

SSNs and ID Theft

Federal Trade Commission Report

December 2008

SSN Reduction – Why?

OMB M-07-16 (2007) and OMB A-130 (2016)

- Agencies shall take steps to eliminate the unnecessary collection, maintenance, and use of SSNs, and explore alternatives to the use of SSNs as a personal identifier.

SSN Fraud Prevention Act (2017)

- An agency may not include the SSN of an individual on any document sent by mail unless the head of the agency determines that its inclusion on the document is necessary.

“Requirements” for SSN Replacement

Functional “Requirements”

- The identifier is meaningless but unique – globally!
- The identifier does not “leak” PII or sensitive information
- Public exposure does not allow its use as an authenticator
- When needed and allowed by policy, can be shared and resolved across systems, agencies and organizations

Non-Functional “Requirements”

- Implementation needs to add value beyond policy compliance!
- Commercially viable such that DHS and USG are not held hostage to a GOTS O&M long tail
- Global standards-based support to ensure interoperability across and availability within diverse future COTS products

W3C Decentralized Identifiers (DIDs)

A meaningless but unique identifier that is:

- Immutable over time
- Globally resolvable
- Privacy respecting
- Cryptographically verifiable

DIDs can be used to identify People, Organization and Things

Decentralized Identifiers (DIDs) v1.0
Core architecture, data model, and representations

W3C Proposed Recommendation 03 August 2021

Scheme

did:example:123456789abcdefghi

DID Method

DID Method Specific String

Example(s)

did:web:www.cbp.gov:trade
did:web:www.uscis.gov:green-card
did:[did method]:123abcde

https://www.w3.org/TR/did-core/

Privacy Case Law Update 2021

November 3, 2021

9:45 AM to 10:45 AM

Panelists

(b) (7)(C) [redacted])

United States Department of Justice, Office of Privacy & Civil Liberties

(b) (7)(C) [redacted]

Central Intelligence Agency, Office of the General Counsel

(b) (7)(C) [redacted]

Federal Bureau of Investigation, Office of the General Counsel, Privacy & Civil Liberties Unit

Standing and Harm

TransUnion v. Ramirez, 141 S. Ct. 2190 (2021)

"No concrete harm, no standing."

Article III of the Constitution limits the jurisdiction of federal courts to "cases" or controversies." To establish Article III standing, a plaintiff must show that they suffered an "injury in fact" – an invasion of a legally protected interest that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."

8,185 individuals with OFAC alerts in their credit files sued TransUnion under the Fair Credit Reporting Act for failing to use reasonable procedures to ensure the accuracy of their credit files. Parties then stipulated that only 1,853 individuals had their misleading credit reports containing OFAC alerts provided to third parties during the 7-month period specified in the class.

Held: "Only plaintiffs concretely harmed by a defendant's statutory violation have Article III standing to seek damages against that private defendant in federal court."

Privacy Act and Alternative Causes of Action

5 U.S.C. § 552a(g)(1)-Civil Remedies

Whenever any agency

(A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

(B) refuses to comply with an individual request under subsection (d)(1) of this section;

(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

Privacy Act and Alternative Causes of Action

Doe v. Chao, 540 U.S. 614, 619 n.1 (2004)

"The Privacy Act says nothing about standards of proof governing equitable relief that may be open to victims of adverse determinations or effects, *although it may be that this inattention is explained by the general provisions for equitable relief within the Administrative Procedure Act (APA), 5 U.S.C. § 706.*" *Doe*, 540 U.S. at 619 n.1 (emphasis added).

Privacy Act and Alternative Causes of Action

Equitable Remedy for Constitutional Violation Claim

Fazaga v. Federal Bureau of Investigation, 965 F.3d 1015 (9th Cir.)

Declaratory Relief under Declaratory Judgement Act

Morinville v. U.S. Patent and Trademark Office, 442 F. Supp.3d 286 (D.D.C.)

Privacy Act and Alternative Causes of Action

Fazaga v. Federal Bureau of Investigation, 965 F.3d 1015 (9th Cir.)

Factual Summary

Plaintiffs, three Muslim residents of Southern California, filed a class action alleging that, between 2006 and 2007, FBI hired a confidential informant to illegally gather information as part of a counterterrorism investigation.

Plaintiffs allege that the confidential informant recorded interactions using audio and video recording devices provided by FBI to surreptitiously record plaintiffs affiliated with area mosques, included conversations in a mosque prayer hall, at homes, in cars, and within offices.

Plaintiffs alleged, among other claims, that these actions constituted unconstitutional activity (e.g., unreasonable searches and chilling First Amendment activities), and a violation of the Privacy Act's prohibition on maintaining records describing First Amendment protected activities.

Privacy Act and Alternative Causes of Action

Fazaga v. Federal Bureau of Investigation, 965 F.3d 1015 (9th Cir.)

Privacy Act Claim

Complaint expressly provides that "[t]he FBI is sued for injunctive relief only." *Fazaga*, 965 F.3d at 1064.

"Plaintiffs cannot obtain injunctive relief except for violations as to which such relief is specifically permitted." *Fazaga*, 965 F.3d at 1064.

Constitutional Violation Claim

"Federal courts have the equitable power 'to order the expungement of Government records where necessary to vindicate rights secured by the Constitution or by statute.'" Fendler v. U.S. Parole Comm'n, 774 F.2d 975, 979 (9th Cir. 1985) (quoting Chastain v. Kelley, 510 F.2d 1232, 1235 (D.C. Cir. 1975))).

"Previous cases involving claims brought under both the Privacy Act and the Constitution did not treat the Privacy Act as displacing a constitutional claim, but instead analyzed the claims separately. And the circuits that have directly considered whether the Privacy Act displaces parallel constitutional remedies have all concluded that a plaintiff may pursue a remedy under both the Constitution and the Privacy Act." *Fazaga*, 965 F.3d at 1054 (internal footnotes omitted).

Privacy Act and Alternative Causes of Action

Morinville v. United States Patent and Trademark Office, 442 F.Supp.3d 286 (D.D.C.)

Factual Summary

Plaintiff claims against the United States Patent and Trademark Office (PTO) stem from a former program called "Sensitive Application Warning System" (SAWS).

Under SAWS, Plaintiff allege that PTO personnel flagged "sensitive applications," which allegedly related to "the possibility for publicity," "objectionable or derogatory subject matter," or "based on the identity of the patent applicant." Once flagged, the patent application allegedly could not be granted until the flag was removed.

Plaintiffs alleged, among other things, that PTO failed to accurately maintain records on the plaintiffs, because plaintiffs' patent files alleged flagged by the SAWS program contained no SAWS material.

In additional to traditional Privacy Act claims, plaintiffs sought relief under the Declaratory Judgment Act seeking a declaration of PTO's violation and the plaintiffs' Privacy Act rights.

Privacy Act and Alternative Causes of Action

Morinville v. United States Patent and Trademark Office, 442 F.Supp.3d 286 (D.D.C.)

Declaratory Judgement Act, 28 U.S.C. § 2201(a)

In a case of actual controversy within its jurisdiction, ... as determined by the administering authority, any court of the United States, upon the filing of an appropriate pleading, may declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought. Any such declaration shall have the force and effect of a final judgment or decree and shall be reviewable as such.

Declaratory Judgement Act Claim

"Ultimately, relief under the Declaratory Judgment Act may be unnecessary, and the Court, in its discretion, may dismiss this claim. However, at the motion to dismiss stage, the Court is not prepared to say that Plaintiffs' Declaratory Judgment Act claim is duplicative of their Privacy Act claims or otherwise unnecessary or inappropriate." *Morinville*, 442 F.Supp.3d at 296.

Privacy Act and the First Amendment

Garris v. FBI, 937 F.3d 1284 (9th Cir. 2019)

Section (e)(7) of the Privacy Act states that "Each agency that maintains a system of records shall maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."

The FBI had two memos in its systems describing First Amendment protected activities of plaintiff as part of an investigation. Plaintiff argued that even if the creation of the memos was acceptable under (e)(7)'s law enforcement activity exception at the time they were written, the FBI could no longer maintain the records once these investigations closed.

9th Circuit panel agrees with plaintiff. "Unless a record is pertinent to an ongoing authorized law enforcement activity, an agency may not maintain it under § (e)(7) of the Privacy Act" (emphasis added).

The court's ruling creates a circuit split with the D.C. Circuit's ruling in MacArthur Foundation v. FBI, (D.C. Cir. 1996).

Facial Recognition and Privacy

ACLU v. Clearview, No. 20-CH-4353 (Ill. Ct. Cl. Cook Cnty. Aug. 27, 2021)

Clearview "scrapes" publicly available databases in order to capture facial images, which it then runs through its facial recognition software. It sells access to its results to subscribers, including law enforcement.

ACLU argued that under Illinois' Biometric Identification and Privacy Act ("BIPA"), Clearview was required to get permission from those whose images it captured/stored.

Clearview argued that BIPA violated the First Amendment.

Court, applying intermediate scrutiny, rejects Clearview's First Amendment argument, denies Clearview's Motion to Dismiss.

Discussion/Q & A

2021 FEDERAL PRIVACY SUMMIT

FPC

NOVEMBER 3, 2021

PROGRAM GUIDE | VIRTUAL EVENT

HOSTED BY THE FEDERAL PRIVACY COUNCIL

TABLE OF CONTENTS

3 **SUMMIT OVERVIEW**
Introduction to the 2021 Federal Privacy Summit

4 **WELCOME**
Message from the FPC Chair

5 **SCHEDULE**
2021 Federal Privacy Summit at a Glance

7 **KEYNOTE PANEL**
Privacy & Equity Panel

9 **BREAKOUT SESSIONS**
Overview of Sessions

12 **FPC AWARDS**
Meet FPC's Award Recipients

14 **PRIVACY SUMMIT FAQS & TECH SUPPORT**

PRIVACY SUMMIT 2021

The Federal Privacy Summit draws privacy professionals from across the Executive Branch. In addition to featuring exciting speakers and topics, this event includes the presentation of FPC Awards, which recognize the extraordinary achievements of Federal privacy professionals. It is free of charge and open to Federal employees and contractors in the Executive Branch.

MESSAGE FROM THE FPC CHAIR

What a year it has been!

Its unprecedented challenges touched every aspect of our lives, including our privacy work. As the nation has struggled to fight the spread of COVID-19 and respond to its impacts, our privacy work has been key, especially with regard to the health and safety of the Federal workplace.

I am proud of our collective response to the pandemic – both in terms of our ability to continue our FPC work and events without missing a beat, as well as our ability to ensure privacy is a central consideration in protecting the federal workforce through vaccinations and workplace safety.

The Federal Privacy Council has remained constant and committed to ensuring that privacy programs continue to evolve and build the trust in government that is central to our democracy – trust that depends on the fair handling of the information about those we serve, even in the most unprecedented of circumstances.

Perhaps one word sums it up best – collaboration! Collaboration has never been more important in data governance – both within our privacy community and with our partners in related disciplines.

Even in a new virtual work environment collaboration has been important to strengthening our community and is evident through our recent growth and cross agency accomplishments over the past year.

I am proud to serve alongside a truly spectacular group of privacy professionals who are skilled at turning challenges into accomplishments and look forward to another successful year ahead!

KIRSTEN MONCADA

FPC Chair and OIRA Privacy Branch Chief, OMB

2021 FEDERAL PRIVACY SUMMIT AGENDA

November 3, 2021

9:00am - 9:15am	Welcome and Logistics	Shenaye Holmes, FPC Senior Advisor, GSA
9:15am - 9:45am	Opening Remarks and FPC awards	Kirsten Moncada, FPC Chair and OIRA Privacy Branch Chief, OMB
9:45am-10:45am	BREAKOUT 1 (choose one)	
	Privacy Case Law Update 2021	***Speakers:*** (b) (7)(C) [redacted] IA DJ FBI
	CNSS and Privacy	***Moderator:*** (b) (7)(C) [redacted] NSA ***Speakers:*** AndraLeigh (Andy) Rodini, DOE (b) (7)(C) [redacted] CIA DNI
	Decentralized Identifiers: How DIDs Can Help Reduce the Use of SSNs as an Authenticator	***Moderator:*** Charlie Cutshall, CFTC ***Speakers:*** (b) (7)(C) [redacted] DHS (b) (7)(C) [redacted] DHS Naomi Lefkovitz, NIST
10:45am -11:00am	BREAK	
11:00 am-12:30 pm	**Keynote Panel: Privacy and Equity** While protecting privacy in our increasingly connected society is no easy task, doing so is more than just an administrative nicety. Instead, as the keynote panel will discuss, privacy is a critical first order right that helps ensure the safety, civil rights, economic stability, and enfranchisement of marginalized communities, while also advancing critical democratic values. In the same way that surveillance can be used to control individuals, privacy can empower them to craft their own identities, resist violence, and shape the public sphere. As a result, whether government agencies are deploying data-centric technologies or regulating them, agencies need to consider the perspectives and privacy needs of marginalized people. ***Panelists:*** Khiara M. Bridges, Professor of Law, UC Berkeley School of Law Scott Skinner-Thompson, Associate Professor, University of Colorado Law School Michele Gilman, Professor of Law, University of Baltimore School of Law ***Moderators:*** Kirsten Moncada, FPC Chair (OMB) Joo Chung, FPC Vice-Chair (DOD)	

2021 FEDERAL PRIVACY SUMMIT AGENDA

November 3, 2021

12:30pm -1:30pm	BREAK	
1:30pm - 2:30pm	BREAKOUT 2 (choose one)	
	NIST SP 800-53A, Revision 5: Latest Updates and Tools for Conducting Effective Control Assessments	***Speakers:*** Alaina Nguyen, PBGC Claire Barrett, NIST Victoria Yan Pillitteri, NIST
	Privacy Risks, Civil Liberties Risks, and Publicly Available Data	***Moderator:*** (b) (7)(C) [redacted] NSA ***Speakers:*** (b) (7)(C) [redacted] ODNI (b) (7)(C) FBI (b) (7)(C) [redacted] DHS
	Negotiating Data Sharing Agreements: Case Studies, Trip-ups, and Tools	***Speakers:*** Debra Danisek, CBP-DHS Maya Bernstein, HHS Megan Metcalf, USAID Todd Anderson, USAID
2:30pm - 2:45pm	BREAK	
2:45pm -3:45pm	BREAKOUT 3 (choose one)	
	The Responsible Collection of Diversity, Equity, and Inclusion Data	***Speakers:*** Suzanne Wachter, USAID Jessica Holzberg, U.S. Census Bureau Darrell Overbey, EEOC Agnes O'Hanlon, USAID
	Identify and Remediate Instances of PII in Free Text	***Moderator:*** Donna Miller, CDC ***Speakers:*** Chad Tompkins, CFPB Travis Hoppe, CDC William Frankenstein, State
	Cross-Border Data Flows and Government Access to Data: Commercial and National Security Perspectives	***Moderator:*** Nasreen Djouini, ITA ***Speakers:*** Clinton Harper, ITA (b) (7)(C) [redacted] ODNI Sam Schofield, ITA

KEYNOTE PANEL: PRIVACY AND EQUITY

11:00 AM - 12:30 PM

While protecting privacy in our increasingly connected society is no easy task, doing so is more than just an administrative nicety. Instead, as the keynote panel will discuss, privacy is a critical first order right that helps ensure the safety, civil rights, economic stability, and enfranchisement of marginalized communities, while also advancing critical democratic values.

In the same way that surveillance can be used to control individuals, privacy can empower them to craft their own identities, resist violence, and shape the public sphere. As a result, whether government agencies are deploying data-centric technologies or regulating them, agencies need to consider the perspectives and privacy needs of marginalized people.

KHIARA M. BRIDGES

Professor of Law,
UC Berkeley School of Law

SCOTT SKINNER-THOMPSON

Associate Professor,
University of Colorado Law School

MICHELE GILMAN

Professor of Law,
University of Baltimore School of Law

MEET THE PANEL

Khiara M. Bridges

Professor of Law, UC Berkeley School of Law

Khiara M. Bridges is a professor of law at UC Berkeley School of Law. She has written many articles concerning race, class, reproductive rights, and the intersection of the three. Her scholarship has appeared or will soon appear in the Harvard Law Review, Stanford Law Review, the Columbia Law Review, the California Law Review, the NYU Law Review, and the Virginia Law Review, among others. She is also the author of three books: Reproducing Race: An Ethnography of Pregnancy as a Site of Racialization (2011), The Poverty of Privacy Rights (2017), and Critical Race Theory: A Primer (2019).

Scott Skinner-Thompson

Associate Professor, University of Colorado Law School

Scott is an Associate Professor at the University of Colorado Law School where he researches constitutional law, civil rights, and privacy law, with a particular focus on LGBTQ and HIV issues. Bringing together these topics, his new book, Privacy at the Margins, examines how privacy can function as an expressive, anti-subordination tool of resistance to surveillance regimes.

Michele Gilman

Professor of Law, University of Baltimore School of Law

Michele Gilman is the Venable Professor of Law and Associate Dean for Faculty Research and Development at the University of Baltimore School of Law. Professor Gilman directs the Civil Advocacy Clinic, where she supervises students representing low-income individuals and community groups in a wide range of litigation, legislation, and law reform matters. She also teaches evidence, federal administrative law, and poverty law. Professor Gilman writes extensively about data privacy and social welfare issues, and her articles have appeared in journals including the California Law Review, the Vanderbilt Law Review, and the Washington University Law Review, as well as in the popular media. She was a faculty fellow at Data & Society in 2019-2020, researching the intersection of privacy law with the concerns of low-income communities. She is the author of Poverty Lawgorithms: A Poverty Lawyer's Guide to Fighting Automated Decision-Making Harms on Low-Income Communities. She received her B.A. from Duke University, and her J.D. from the University of Michigan Law School.

9:45AM BREAKOUT SESSIONS

(CHOOSE ONE)

PRIVACY CASE LAW UPDATE 2021

SPEAKERS: (b) (7)(C), (b) (6) [redacted]

Building off of last year's publication of the Overview of the Privacy Act of 1974, 2020 Edition, please join this distinguished panel of Privacy Act and privacy law experts as they review and analyze significant privacy case law impacting the Federal privacy community. In addition to legal analysis of court decisions interpreting the Privacy Act of 1974, 5 U.S.C. § 552a (2018), this panel will also discuss significant privacy case law in emerging areas of interest. Whether you are new to the privacy profession, or a seasoned privacy professional, the privacy case law discussion is a popular panel not to be missed!

CNSS AND PRIVACY

MODERATOR: REBECCA RICHARDS, NSA
SPEAKERS: ANDRALEIGH (ANDY) RODINI, DOE, (b) (6), (b) (7)(C) [redacted]

Come learn how CNSS is approaching the division of privacy baseline controls and privacy overlays. The Committee for National Security Systems (CNSS) reviews and adapts NIST 800-53 guidance for national security systems. This guidance CNSSi 1253 is used by agencies with national security systems, but also more broadly by the Department of Defense whether the system is NSS or not. With the Rev 5 out, CNSS has been updating its instruction with an updated and integrated approach to privacy and security. CNSS issued Privacy Overlays in 2015 that are applied to systems processing PII. With Revision 5, CNSS is going to be issuing both security and privacy baseline controls and privacy overlays. This panel will discuss the approach taken to determine baseline, privacy implementation consideration, and overlay.

DECENTRALIZED IDENTIFIERS: HOW DIDS CAN HELP REDUCE THE USE OF SSNS AS AN AUTHENTICATOR

MODERATOR: CHARLIE CUTSHALL, CFTC
SPEAKERS: (b) (6), (b) (7)(C) [redacted] NAOMI LEFKOVITZ, NIST

We will use the conversation to explore the use of decentralized identifiers and how it can help separate identifiers from authenticators.

1:30 PM BREAKOUT SESSIONS

(CHOOSE ONE)

NIST SP 800-53A, REVISION 5: LATEST UPDATES AND TOOLS FOR CONDUCTING EFFECTIVE CONTROL ASSESSMENTS

SPEAKERS: ALAINA NGUYEN, PBGC, CLAIRE BARRETT, NIST, VICTORIA YAN PILLITTERI, NIST

Are you ready to learn the latest updates on NIST Special Publication (SP) 800-53A Revision 5 and add some tools to your assessment toolbox? In this session, hear how SP 800-53A can help agencies build effective control assessment plans using the recently integrated security and privacy control catalog (SP 800-53), assess and monitor the effectiveness of implemented controls efficiently, and interpret control assessment results in ways that provide meaningful insights to their organizations' overall risk posture. You will also hear from federal privacy and security professionals about automated tools that are helping their organizations carry out and manage these control assessment functions efficiently.

PRIVACY RISKS, CIVIL LIBERTIES RISKS, AND PUBLICLY AVAILABLE DATA

MODERATOR: REBECCA RICHARDS, NSA
SPEAKERS: (b) (7)(C) [redacted]

Learn about the benefits and risks to reviewing and collecting publicly available information in the context of law enforcement, homeland security, and intelligence activities and how you might apply these lessons learned to your agency. What is publicly available information, when and how does the Privacy Act apply, and what questions should you be asking to keep your agency following best practices?

NEGOTIATING DATA SHARING AGREEMENTS: CASE STUDIES, TRIP-UPS, AND TOOLS

SPEAKERS: (b) (7)(C) [redacted], MAYA BERNSTEIN, HHS, MEGAN METCALF, USAID, TODD ANDERSON, USAID

Data Sharing Agreements describe and govern the sharing of sensitive information between agencies in order to facilitate access and implement adequate safeguards. This session will highlight essential elements of data sharing agreements, useful governance processes, and particular sensitivities such as restrictions on use and further disclosure, derivative work products, and re-identification. We will discuss two or more illustrative examples, including USAID and CBP's sharing of demographic data on Central American citizens who are migrants, and the sharing of COVID-19 data to support work under the public health emergency.

2:45PM BREAKOUT SESSIONS

(CHOOSE ONE)

THE RESPONSIBLE COLLECTION OF DIVERSITY, EQUITY, AND INCLUSION DATA

SPEAKERS: SUZANNE WACHTER, USAID, JESSICA HOLZBERG, U.S. CENSUS BUREAU, DARRELL OVERBEY, EEOC, AGNES O HANLON, USAID

Requests for collection of diversity, equity and inclusion data are increasing with recent executive orders. At USAID, we've had requests to collect this type of information both internally within our staff and internationally as our partners look to ensure our programming is reaching vulnerable populations. We'd like to have a discussion with all of our agency stakeholders on the pitfalls, best practices, and authorities we've identified relevant to these data collection initiatives.

IDENTIFY AND REMEDIATE INSTANCES OF PII IN FREE TEXT

MODERATOR: DONNA MILLER, CDC

SPEAKERS: CHAD TOMPKINS, CFPB, TRAVIS HOPPE, CDC, (b) (6) [redacted]

Automating a system to assist in the detection and removal of PII in free text is a shared problem across many agencies. Releasing data to the public is often in conflict with privacy and disclosure risk. This panel session w ll cover three explicit processes and systems from the CDC, CFPB, and the State Department. The panel will cover technical and policy implementation challenges, address the trust and safety of automated solutions, and discuss use cases beyond the original implementations.

CROSS-BORDER DATA FLOWS AND GOVERNMENT ACCESS TO DATA: COMMERCIAL AND NATIONAL SECURITY PERSPECTIVES

MODERATOR: NASREEN DJOUINI, ITA

SPEAKERS: CLINTON HARPER, ITA, (b) (6), (b) (7)(C) [redacted], SAM SCHOFIELD, ITA

This panel will discuss global trends in data protection and why the interoperable mechanisms to bridge gaps between disparate regulatory regimes and across geographies is integral to enabling modern trade, protecting national security priorities, and regulating emerging digital technologies. The panel will cover the following topics: 1) high-level overview of cross-cutting commercial and national security issues in data privacy; 2) update on efforts to negotiate an enhanced EU-U.S. Privacy Shield Framework and alternative, interoperable data privacy frameworks promoted by the USG; and 3) discussion of ongoing multilateral dialogues (e.g. OECD) with like-minded democracies to address national security concerns and rules for government access associated with processing of personal data and cross-border data transfers.

2021 FPC AWARDS

DEPARTMENT OF DEFENSE (DOD) PRIVACY TRAINING TEAM

The team has made exceptional contributions to the field of Privacy which have significantly advanced the role of privacy inside and outside the Department of Defense through the creation of a live virtual training series.

LYN M. KIRBY

CINDY STANLEY

MARY FLETCHER

VIKI HALABUK

TRACY C. ROGERS

CHERYL JENKINS

ERNEST G. TAYLOR

2021 FPC AWARDS

AWARD FOR EXCELLENCE

In recognition of her distinguished career in government and service to the federal privacy community, we are pleased to honor Maya Bernstein. Maya is known across government and in the privacy profession as a keen analyst, an effective negotiator, a practical problem solver, and a mentor to junior staff. Her insights have contributed to program improvements affecting practically every agency of government and the safeguarding of privacy rights across many sectors.

MAYA BERNSTEIN

DEPARTMENT OF HEALTH AND HUMAN SERVICES

PRIVACY SUMMIT FAQS

How do I join the day of the event?

- On November 3, 2021 please log onto the Zoom Gov link at 8:45 am
  - Please note, participants will be placed in a waiting room before the event so it is pivotal to join early
- Please refer to this website if you find yourself having trouble logging on

Does this event qualify for IAPP CPE credits?

- Yes, participants are eligible for IAPP CPE credits, which are awarded to CIPP, CIPM and CIPT holders who attend events, forums and online programs that are provided by other organizations and agencies. Participants may submit 1 CPE per event hour attended using the online CPE Submission Form within 90 days of the event.

Will the event be recorded?

- No, the 2021 Federal Privacy Summit will not be recorded.

Is this event open to the press?

- No, the 2021 Federal Privacy Summit is not open to the press.

Can I call into the event?

- Participants are strongly discouraged from calling into the event and should only use the feature as a last resort.
- If absolutely necessary, participants must link their participant ID. Participants who do not link their participant ID will be removed from the Summit.
- Where can I find my participant ID?
  - Please click here for information on where you can find your participant ID

Can I leave and come back?

- Participants are encouraged to remain in the Summit for the entire day and not exit out of the zoom link during breaks.
- If participants do leave, they will be placed back into a waiting room where they will be re-approved before entering the Summit.

TECH SUPPORT

I am having trouble accessing the room links in ZoomGov.

- Please try to access ZoomGov from a different browser, turn off your VPN, contact your IT, or use a personal device.
- When prompted after following the ZoomGov link, select "Join from Browser." Attendees do not need to download the Zoom Desktop Client in order to participate.
- When prompted to connect audio, select "Join with Computer Audio" or "Call Me" to have the system call your phone.
- Entry for the summit will require host approval from a waiting room so please join early.

I can't seem to unmute myself or turn on my video in ZoomGov.

- Participants will be muted upon joining and will not have the ability to unmute or turn on their video, unless prompted by the moderator.

How many Zoom links will there be?

- Participants will use a Zoom Gov link to participate in the Summit. Participants will access a seperate zoom webinar link to attend the keynote panel on privacy and equity.

How do I choose what breakout sessions I would like to attend? Will I need a separate Zoom Link?

- When it is time for the breakout sessions, participants will be able to self select the session they would like to join by clicking on the option they see on their screens.

Do I need to use my Government issued Zoom Account?

- Participants are strongly encouraged to use their government zoom account. Participants are REQUIRED to change their Zoom name to [First, Last (Agency)] upon entry ex: [Sari Wilson (GSA)]
- Unidentified participants will be REMOVED from the Summit and will not be allowed to return.

ZOOM GOV MEETING INFO

2021 Federal Privacy Summit (Zoom Gov Room):

Please use the below link to access all summit events with the exception of the keynote panel.

(b) (6)

Keynote Panel: Privacy & Equity (Zoom Webinar):

Please use the below link to access the Keynote Panel on Privacy & Equity.

(b) (6)

Interagency Data Sharing
Federal Privacy Council Summit

U.S. Agency for International Development
U.S. Customs and Border Protection
Department of Health and Human Services

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

- The information provided in this slide deck is for informational purposes only and should not be understood as legal advice.
- This presentation is only for US Government Distribution.
- The opinions expressed are personal opinions of the speakers, and not of their respective agencies.

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

Best Practices For Data Sharing

- ★ Streamlining data requests before beginning MOU process
- ★ Involve subject matter experts from the beginning
- ★ Assess at the outset whether the data can be shared
- ★ Open lines of communication
- ★ Ensure nexus between problem to be solved and data requested

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

Case Study Discussion

1. CBP/USAID Case Study
2. HHS Case Study

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

Common Elements of Data Sharing Agreements (1 of 5)

- Introductory Information:
  - names of the entities sharing and receiving data
  - type of agreement (data sharing, data use, or MOU)
- Purpose and Scope:
  - identify the parties involved
  - identify program, activity, goal to be achieved
  - description of data to be shared
  - specific intended products or deliverables.

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

Common Elements of Data Sharing Agreements (2 of 5)

- Governing Authorities: Authorities are likely to differ depending on the nature of the data and purpose of the agreement.
  - each party's respective authorities to share or receive the data
  - other governing authorities that impact the data use, sharing, and restrictions
- Description of Data to be Exchanged:
  - subject matter of data
  - specific data elements
  - sensitivities of data as a group, or particular elements
  - source of data
  - format of data

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

Common Elements of Data Sharing Agreements (3 of 5)

- Permissible Uses and Limitations
  - permissible uses of the data
  - restrictions on use and further disclosure
  - data rights and licensing restrictions or allowances, if any
  - privacy considerations, privacy risk mitigations (e.g. derivative work products, re-id prohibition, SORN, contract clauses, PIA)
- Retention:
  - limitations on recipient retention (e.g. original retention period)
  - audits of retention compliance
  - attestation of compliance with retention requirements

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

Common Elements of Data Sharing Agreements (4 of 5)

- Responsibility for Costs:
  - Each party's responsibilities under the agreement
- Data Transfer and Storage:
  - technical description and details for how data will be shared and stored
- Safeguards:
  - information security protections and safeguards
  - approach agreed upon for handling suspected or actual security incident or data breach

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

Common Elements of Data Sharing Agreements (5 of 5)

- Duration, Modification, and Termination of the DSA:
  - Duration of Agreement and amendments
  - Disposition of data after termination
- Points of Contact:
  - Name, email, phone for questions or trouble shooting agreement
- Disclaimer
  - Any legal disclaimers for the agreement
- Signatures:
  - Records the concurrence of the parties

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

Helpful Data Assessment Questions (part 1)

- ❑ Is there PII in the data? Was there PII that is now aggregated or anonymized?
- ❑ What is the purpose of sharing the data? Is it necessary and relevant for the project/activity?
- ❑ Is the data marked (e.g., CUI markings) or may be appropriate to add before sharing?

- ❑ Were the data collected using informed consent? How does the language of the consent impact the ability to share the data?
- ❑ What particular sensitivities are there in the data (e.g. law enforcement, substance use treatment, domestic violence, other?)

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

Helpful Data Assessment Questions (part 2)

- ❑ Is any of the data classified (confidential, secret, top secret, etc)?
- ❑ What intellectual property or other rights or restrictions are applicable?
- ❑ What contractual provisions apply to this data?
- ❑ What documents must be incorporated by reference to your agreement? (e.g. contracts, assistance awards, previous agreements, user agreements)
- ❑ What are the U.S. and international best practices for sharing this type of data, to the extent that the data sharing issues are not covered by law?

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

Panel

Megan Metcalf, USAID, mmetcalf@usaid.gov

Maya A. Bernstein, HHS, maya.bernstein@hhs.gov

Todd M. Anderson, USAID, tanderson@usaid.gov

(b) (7)(C), CBP, (b) (7)(C)

US GOVERNMENT ONLY - NO FURTHER DISTRIBUTION

Identify and Remediate Instances of PII in Free Text

(b) (6) [redacted]
Senior Data Scientist
Department of State, Center for Analytics

FOIA Privacy Concerns

Department of State Center for Analytics Partnership

Challeng

- Department official e records contain significant amount of personal information

Approach

- Partnership with Bureau of Administration Privacy Office to implement data science solutions, **message tag model** and **PII detection model**

Impact

- **Message Tag Model:** Reduces up to 75% of irrelevant emails for official review
- **PII Detection:** Enables Privacy Officer review to focus on <1% of relevant emails

Message Category Model

- Automatically tag e-mails as “Personal” or “News Clippings” with 90% accuracy
- Support Vector Machine with linear kernel functions identified as best performing models
- Privacy, FOIA office collaboration with IRM (DoS IT) and Center for Analytics validation of results

PII Detection

- Records may contain PII, Health Information, or Financial Information
- Combination of RegEx, OCR, Entity Resolution identify topics of concern
- Collaboration with Privacy Office identified policy changes and recommendations going forward

What’s Next

Department of State Center for Analytics Collaborations on Privacy

Disclosure Analytics

- Additional tools to support Privacy Office efforts, combinations of PII detection

Differential Privacy Approaches

- Identify approaches to enhance internal data sharing within the Department

Model Monitoring and MLOps

- Balancing infrastructure upgrades, assessing ongoing accuracy of deployed models, and nature of new records

Identify and Remediate Instances of PII in Free Text

Travis Hoppe
Chief Data Scientist
CDC, National Center for Health Statistics

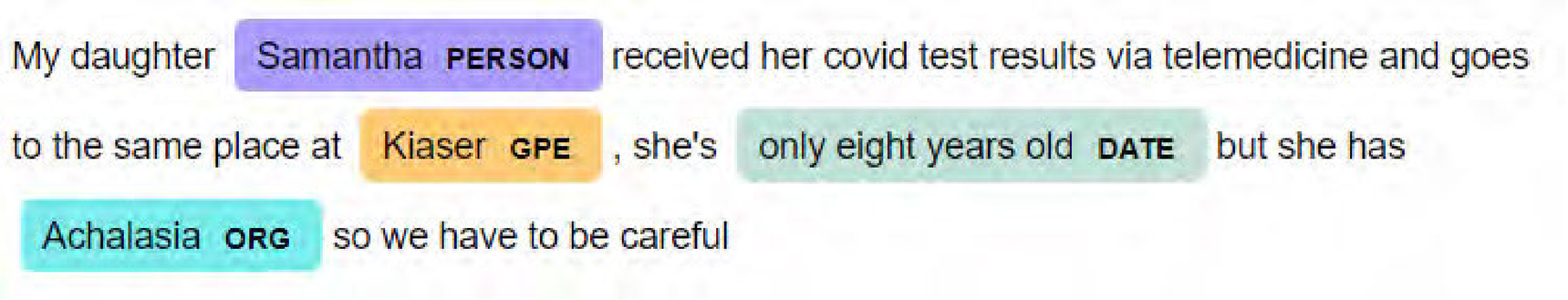
The findings and conclusions in this presentation are those of the author and do not necessarily represent the official position of the Centers for Disease Control and Prevention.

Detecting PII is difficult and situational

My daughter Samantha received her covid results via telemedicine and goes to the same place at Kiaser. She's only 8 years old but she has Achalasia so we have to be careful.

- Only 1-2 pieces of direct PII (name & age)
- Rare condition or diseases
- Hospitals & insurance companies often need to be identified (no comprehensive list)
- Typos and grammatical errors usually present
- Limited ability to install software
- **Needed 100% recall for our use-case**

spaCy: Named Entity Recognition



- spaCy returns results as code for automating known false positives (e.g., political figures)
- Results were visualized for edge cases
- Recognized: People, Organizations, Locations, Dates, Times, Money, and Geopolitical Entities
- Importantly, improper NER classes (Kiaser:GPE, Achalasia:ORG) still useful for indirect PII
- Combining spaCy approach w/other automated solutions

Identify and Remediate Instances of PII in Free Text

Chad Tompkins
Section Chief, Data and Governance
Consumer Financial Protection Bureau

This presentation is being made by a Consumer Financial Protection Bureau representative on behalf of the Bureau.

It does not constitute legal interpretation, guidance or advice of the Consumer Financial Protection Bureau. Any opinions or views stated by the presenter are the presenter's own and may not represent the Bureau's views. This document was used in support of a live discussion. As such, it does not necessarily express the entirety of that discussion nor the relative emphasis of topics therein.

Consumer Financial Protection Bureau Complaint Process

Consumer Financial Protection Bureau Scrubbing Process

Auto Scrub › Human Review › 100% QA › Company Respons e › Final Check & Publish

Cross-Border Data Flows and Government Access to Data:

Commercial and National Security Perspectives

Panelists

Nasreen Djouini, Moderator

Senior Policy Advisor

Department of Commerce – International Trade Administration

Nasreen.Djouini@trade.gov

Sam Schofield, Panelist

International Trade Specialist

Department of Commerce – International Trade Administration

Sam.Schofield@trade.gov

Clinton Harper, Panelist

Policy Advisor & Administrator

Department of Commerce – International Trade Administration

rade.gov

(b) (6) [redacted], Panelist

Principal Deputy Chief

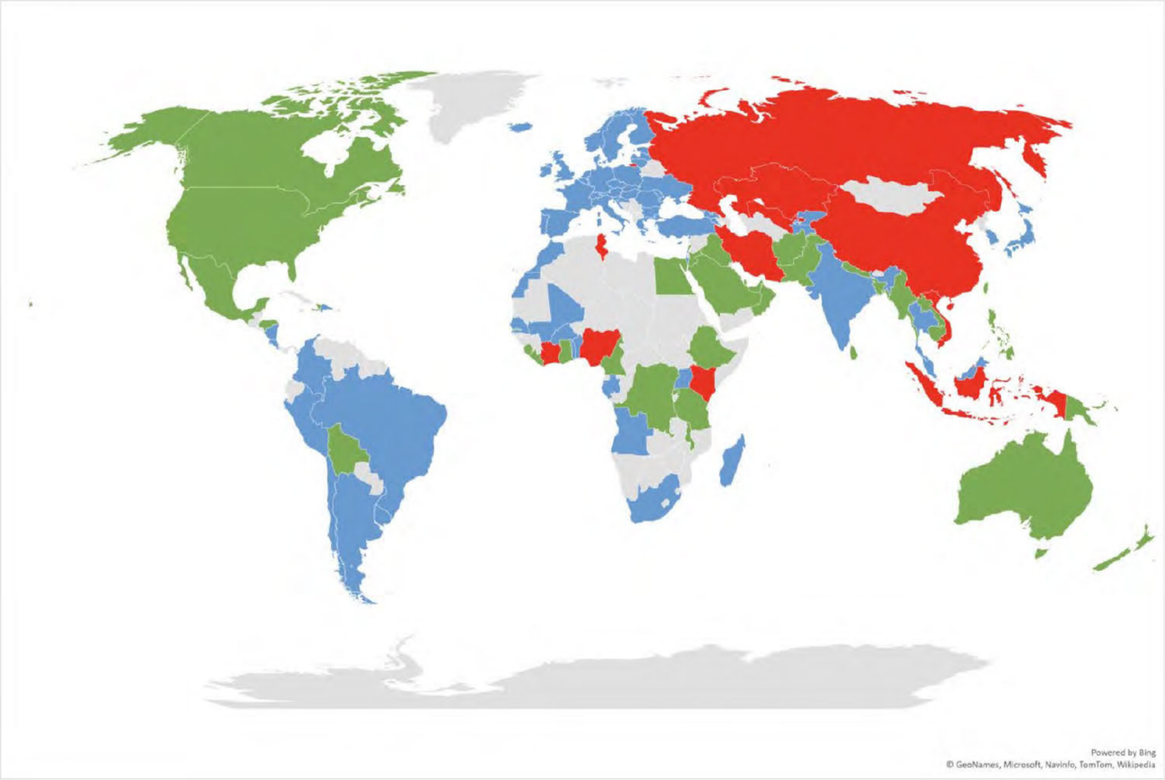
Office of Civil Liberties, Privacy, and Transparency

Office of the Director of National Intelligence

(b) (6) [redacted]

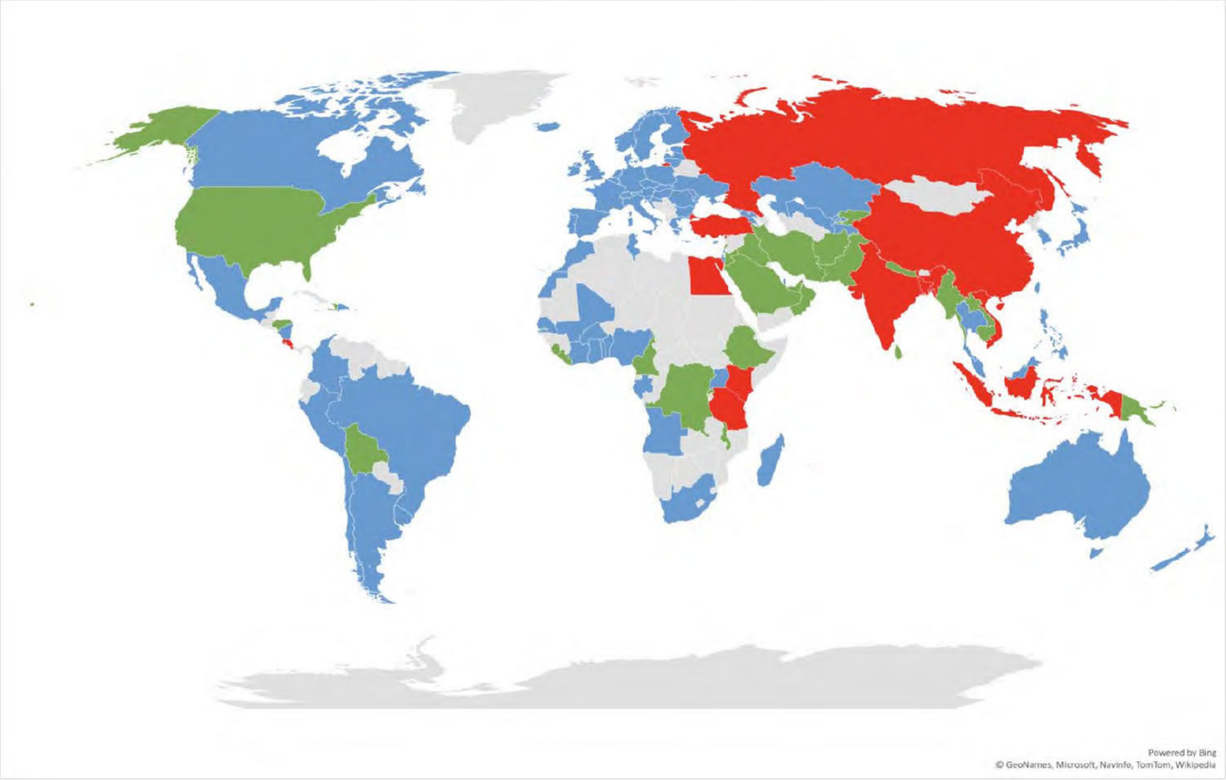
Data as a Non-Universal Concept

Figure 1: World map of data models for cross-border data flows, 2019



Open model **Conditional model** **Control model**

Figure 2: World map of data models for domestic data processing, 2019



Open model **Conditional model** **Control model**

Source: Ferracane and van der Marel (2021), WDR (2021), VoxEU.

APEC Privacy Landscape

APEC Privacy Principles

- Set of principles created to establish effective privacy protections in the APEC region.

2005

2011

- CBPR System established and endorsed.
- Based on the APEC Privacy Principles

2015

- PRP System established and endorsed.
- APEC Privacy Principles Updated

2020

- 9 participating economies
- 8 Accountability Agents (5 in U.S.)
- Working to expand CBPRs outside of APEC

Growth of the APEC CBPR System

The CBPR and PRP system has experienced significant growth in adoption since 2011:

Nine (9) Members	Nine (9) Accountability Agents
➢ United States ➢ Canada ➢ Mexico ➢ Japan ➢ Singapore ➢ Chinese Taipei ➢ Australia ➢ Republic of Korea ➢ Philippines	➢ Established across five (5) member economies ➢ Four (4) established in the last year ➢ Five (5) U.S.-based accountability agents

Cross-Border Data Flows and Government Access to Data:

Commercial and National Security Perspectives

The Importance of U.S.-EU Data Flows

Cross-border data flows are vital to the
$7.1 trillion transatlantic economic relationship.

- Volume of U.S. data flows with the EU is highest in the world.
- EU is the destination of two-thirds of U.S. digital media & services exports.
- U.S.-EU data flows enable:
  - U.S. COMPANIES IN ALL SECTORS *to enhance business operations & innovation.*
  - U.S. CONSUMERS *to benefit from an ever-growing number of goods & services.*
  - U.S. STARTUPS & SMES *to access EU markets at an unprecedented rate.*
  - U.S. EMERGING TECHNOLOGIES *like A.I. & blockchain.*

Cross-Border Data Flows and Government Access to Data:

Commercial and National Security Perspectives

Audience Q&A

Panelists

Nasreen Djouini, Moderator

Senior Policy Advisor

Department of Commerce – International Trade Administration

Nasreen.Djouini@trade.gov

Sam Schofield, Panelist

International Trade Specialist

Department of Commerce – International Trade Administration

Sam.Schofield@trade.gov

Clinton Harper, Panelist

Policy Advisor & Administrator

Department of Commerce – International Trade Administration

rade.gov

(b) (6) [redacted]

Panelist

Principal Deputy Chief

Office of Civil Liberties, Privacy, and Transparency

Office of the Director of National Intelligence

(b) (6) [redacted]

CNSS and Privacy

Moderator: Rebecca "Becky" Richards, NSA

Panelists: (b) (7)(C), ODNI
(b) (7)(C), CIA
Andraleigh "Andy" Rodini, DOE

Committee for National Security Systems (CNSS)

- Interagency group that sets cybersecurity policies for National Security Systems (NSS);
- Comprised of tri-chair: DoD, ODNI, and Civilian Agency.

CNSSI 1253, “Security Categorization and Control Selection for NSS”

- Provides national security programs with guidance on the first and second step of the Risk Management Framework (RMF):
  - Categorize the criticality of the information and system
  - Select the controls.

Adopts and modifies NIST800-53 for NSS:

- NIST SP 800-53, “Security and Privacy Controls for Information Systems and Organizations”
- NIST Special Publication (SP) 800-53B, “Control Baselines for Information Systems and Organizations”
- Differences: No high watermark for NSS

CNSSI 1253 is comprised of:

- Baseline controls for all systems and
- Overlays to include the Privacy Overlays.

CNSS Working Groups

- Safeguarding Working Group
  - Security and Privacy Combined

- Privacy Sub-Working Groups:
  - Privacy Experts from across different agencies including: ODNI, CIA, DoD, NSA, DHA, DLA, VA, DOE, DHS, OMB, and others along with guidance from NIST;
  - Base CNSSI-1253 Document Integration;
  - Privacy Overlay.

CNSSI 1253 Approach to Privacy Controls

- Identify controls as:
  - Privacy Baseline;
  - Privacy Implementation Considerations (PIC);
  - Privacy Overlay.
- Write guidance for beginning of 1253 document explaining the relationship between the security control baseline, privacy control baseline, PIC, and privacy overlay.

CNSSI 1253 – Privacy Baseline

- Identify controls for the Privacy Baseline that are for all systems whether the system maintains PII or Not.

- Example: Risk Assessment (RA-3):

  a) Conduct a risk assessment, including:
     - Identifying threats to and vulnerabilities in the system and determining the magnitude of harm from unauthorized access, and
     - Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

CNSSI 1253 - Privacy Implementation Considerations (PIC)

- Privacy not required but if security chooses it may have privacy implications

  - Example: Monitoring Physical Access PE-6 (3):
  - Physical and Environmental Protection
    a) Employ video surveillance of [Assignment: organization-defined operational areas];
    b) Review video recordings [Assignment: organization-defined frequency]; and
    c) Retain video recordings for [Assignment: organization-defined time period].

CNSSI 1253 - Privacy Overlay

- For systems designed to process PII.
- Example: Risk Assessment (RA-8)

a) Conduct privacy impact assessments for systems, programs, or other activities before.

   a) Developing or procuring information technology that processes personally identifiable information; and

   b) Initiating a new collection of personally identifiable information that:

      1. Will be processed using information technology; and

      2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals.

CNSSI 1253 Table D-1 Awareness and Training (AT)

ID	Title	Privacy Control Baseline	Privacy Implementation Considerations	Security Control Baselines									Justification for NSS Baseline(s)	ODV	Tailoring Considerations		
				Confidentiality			Integrity			Availability							
				L	M	H	L	M	H	L	M	H			Assurance	Resiliency	AT&CK
AT-1	Awareness and Training Policy and Procedures	X															
AT-2	Literacy Training and Awareness	X															
AT-2(1)	Practical Exercises																
AT-2(2)	Insider Threat		√														

CNSSI 1253 – Privacy Baseline

Example: Contingency Planning: Policies & Procedures (CP-1):

A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
   - Contingency planning policy that:
     a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
     b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   - 2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

C. Review and update the current contingency planning:
   - 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
   - 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

CNSSI 1253 - Privacy Implementation Considerations (PIC)

Example: Asset Monitoring - (PE-20)

- Employ [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas].

CNSSI 1253- Privacy Overlay

Example: Authority to Process Personally Identifiable Information (PT-2)

- Determine and document the [Assignment: organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; and
- Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is authorized.

Goals

- The privacy overlays provide a baseline level of protection so that when information is shared between systems, it is readily understood what safeguards were chosen based on the overlay.
- Advance an IC-wide consistent approach on privacy safeguards within cybersecurity.
- Institutionalize privacy into the IC implementation of the RMF.
- Catalyze a culture shift to normalize privacy risk management in the IC.
- Reduce overall privacy risk for individuals and organizations while enabling system owners to make better risk management decisions.

Questions

Backup

CNSSI 1253- Privacy Baseline

Example: Media Protection - (MP-1)

A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
    - 1. [Selection (one or more): organization-level; mission/business process-level; system-level] media protection policy that:
        - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    - 2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;

B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; and

C. Review and update the current media protection: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

CNSSI 1253- Privacy Implementation Considerations (PIC)

Example: System Monitoring – Wireless Intrusion Detection (SI-4(14))

A. Analyze communications traffic and event patterns for the system;
B. Develop profiles representing common traffic and event patterns; and
C. Use the traffic and event profiles in tuning system-monitoring devices.

CNSSI 1253- Privacy Overlay

Example: Information Exchange (CA-3)

- Approve and manage the exchange of information between the system and other systems using
  - Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement];
  - Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
  - Review and update the agreements.

CNSSI 1253 - Privacy Overlay

Example: Security and Privacy Architectures (PL-8)

A. Develop security and privacy architectures for the system that:
   1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
   2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
   3. Describe how the architectures are integrated into and support the enterprise architecture; and
   4. Describe any assumptions about, and dependencies on, external systems and services;

B. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; and

C. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.