DPIAC MEETING MINUTES
September 19, 2017

12:45 p.m. - 12:50 p.m.

Roll Call

Sandra Taylor (Designated Federal Official, Data Privacy and Integrity Advisory Committee)

- N/A
- On phone:
  - Dr. Susan Barber
  - Melanie Gates

12:50 p.m. - 12:55 p.m.

Opening Remarks

Lisa Sotto (Chair, DPIAC)

- Describing today's agenda

1:00 p.m. - 1:15 p.m.

Remarks by the Chief Privacy Officer

Sam Kaplan (Chief Privacy Officer, DHS Privacy Office)

- Salutations
- Describe personal history
  - DOJ, ATF
  - PCLOB
- Describe today's taskings
- Initial strategic thoughts re: PRIV
  - PRIV supports all 5 core DHS missions
    - Prevent terrorism
    - Secure borders
    - Enforce immigration laws
    - Safeguarding cyberspace
    - Disaster response
  - Plan to conduct internal review of PRIV
  - FOIA
    - Work against backlog
  - P/O
    - Conduct PCRs; quantify compliance

- ▪ Screening/vetting
- ▪ Data breach prevention and response
- Compliment prev. work of DPIAC
- Welcome and thank you

1:20 p.m. - 1:35 p.m.

Privacy Office Updates

Jonathan R. Cantor (Deputy Chief Privacy Officer, DHS Privacy Office)

- Salutations
- Staffing updates
  - o Christa Jones
  - o Lara Ballard
  - o Nicole Barksdale-Perry
  - o Roman Jankowski
  - o Margot Hammer
  - o Michael Capparra
  - o Bruce George
  - o Currently recruiting
    - ▪ Sen. Dir. For Privacy Compliance
    - ▪ FOIA Analysts
    - ▪ Privacy Analysts
    - ▪ Admin
- CBP Biometric Exit Program meeting w/advocacy orgs
- FPC Talent Summit
  - o Released FPC HR Toolkit
- Other training and speaking events
- Compliance Updates
  - o PIA/SORNs published
  - o DHS has highest PIA/SORN score in government
  - o Key PIAs
    - ▪ TECS
    - ▪ FEMA deployment tracking system (DTS)
    - ▪ CVM
    - ▪ DHS information notice exchange (INE)
    - ▪ 3 updates to CBP facial recognition pilots
- P/O Updates
  - o Privacy incident breach response guidance updates
  - o PCRs
    - ▪ SOPs + Directive Instruction
    - ▪ USSS
      - Similar to OCHCO PCR
  - o EO Guidance Memo
  - o DHS Instruction Component Privacy Officer

- IS3 Updates
  - CMA
    - Publish matching activity report
      - E.g. FEMA-HUD, most likely will be used to give benefits for Harvey/Irma
  - DARC
  - Insider threat
  - UAVs
  - International information sharing
  - Fusion centers
  - Intelligence product review
- FOIA
  - Restructuring to increase efficiency, compliance with FOIA law updates
  - Processed 40% of DHS backlog
- Thanks and welcome

- Q/A
  - Lisa Sotto: Sounds like not really a change in PRIV's productivity and level of importance despite other changes in fed Government, is that true?
    - JRC: Transition seems typical.
    - LS: Great to hear.
    - SK: because PRIV was created w/creation of DHS, PRIV is more of an institution in DHS than other executive agencies.
    - LS: DPIAC has always thought PRIV = most effective privacy office in fed government, and we've thought other offices try to emulate PRIV.
  - Pete Sand: can you speak more about privacy committee in fed government?
    - SK: think PRIV is a leader in the fed privacy community. PRIV is singularly unique; e.g. DOJ is singularly focused on one mission, but it's a LE agency, benefits agency, intelligence agency, etc. all under one roof so its operations are different. But the institutional advantage is key.
    - JRC: PRIV certainly has institutional advantages in things like budget, etc.
  - Jim Adler: CPO's motivation for comments such as using metrics measuring program effectiveness.
    - SK: Knowing how effective a program is important to policymakers, e.g. for resource management.
  - Sharon A.: Do you envision any change in how PRIV will leverage DPIAC.
    - SK: This is my first time with a FACA. Excited about DPIAC's subject matter expertise. It's an opportunity both for us and Components. It's better government and better policymaking.
  - Lisa Sotto: One thing we've always offered is "an hour's worth of advice" on a call.
    - SK: Appreciate the offer, looking forward to leveraging the expertise.

1:40 p.m. Break (Please return by 1:50 p.m.)

2:00 p.m. - 2:30 p.m.

Biometric Travel Security Initiative

Michael Hardin (Director, Entry/Exit Policy and Planning, Office of Field Operations, U.S. Customs and Border Protection)

Breanne Goodell (Branch Chief, Privacy Compliance, Privacy and Diversity Office, U.S. Customs and Border Protection)

- Lisa Sotto: a few housekeeping items
  - Public comments, sign up outside
  - Intro briefing
- MH
  - We're the Office of Field Operations, people in blue uniforms at airports/ports
  - What that means is that we have a dual-hat mission:
    - Law enforcement
    - Making sure travel flows smoothly
  - Entry/exit office is charged with building a biometric exit system
    - History: 1996, Congress passes law requiring it
    - But departure infrastructure not built with exit checks in mind
    - 9/11 happened
    - 9/11 Commission discovered that several hijackers overstayed their visas
      - Recommended biometric exit system (p.386)
    - 2004-2006/07 built biometric entry system
      - Exit system pilots didn't work very well
    - Technology is now allowing us to build the biometric collection systems
      - Interim systems utilized biographic information
      - E.g. names from passenger manifests
    - So currently: we have biometric entry, biographic exit
      - Biometric entry limited to aliens, visitors
      - Even there, there were exceptions, e.g. children
  - Biometric exit is complicated
    - Cannot interfere with commercial boarding procedures
    - Constraints suggest using other modalities
  - Q (Joanne Mcnabb): does it have to be same modality in as out?
    - A (MH): no
    - Q (JM): but how would you match in without?
    - A (MH): we'd be collecting the out info when they enter.
  - Traditional methods to match biometrics
    - One-to-One: matching one collected identity is the one identity in question
    - One-to-Many: e.g. in crime scene, matching one collected with a database
      - Prev. technologically not feasible

- Therefore: One-to-Few method
    - Using ADIS database to narrow down population
  - Pilots:
    - Jet Blue: face becomes ticket
  - Q (Jim Adler): checking whole flight against bad guy database?
    - A (MH): we're doing that already w/biographic information, not running face against it because it's unreliable and we're already doing it through other means
  - Q (Lisa Sotto): how reliable is it? Because I had to use it yesterday on Delta and it didn't work.
    - A(MH): about 90%. (Delta's not ours.) We currently have an alternate process. Hoping end state gets it down to 2% unreliability.
  - Q (Toke Vandervoort): Where are you getting the pictures from?
    - A(MH): photos we're building our gallery from are from US passport database. For US citizens, we have your passport. For non-US citizens, USCIS. So we already have the pictures.
  - Q (Lynn Goldstein): Are you also taking photos on entry?
    - A(MH): not for US citizens. Yes for non-US citizens. An officer in a booth will take their picture.
    - Q(LG): does this solve your problem with overstaying/terrorism?
    - A(MH): not our role to question duly passed laws from Congress. We think it gives us immigration and counterterrorism benefits. We trust in Congress and 9/11 Commission.
  - Q (SDM): they're using reference points. And unsuccessful fingerprints could be because the screen is dirty.
    - A(MH): that's why we're moving away from fingerprints.
  - Q (Jim Adler): policy to address false negative or false positives?
    - A(MH): we're still working on it—currently only working w/a small sample size. On false positives it's hard because we wouldn't know.
  - Q (Robyn Greene): When you're looking at false positives/negatives, are you evaluating based on disparate impact?
    - A(MH): we are looking at it. We need to do more testing because we only have a small sample size so far, but we haven't seen it yet.
    - Q(Breanne Goodell): follow-up—what problems have you faced?
      - A(MH): camera failing to catch an image.
  - Q (Robert Sloane): you can't get both the false positive and negative to get zero. Question is, are you going to apply to land crossings?
    - A(MH): starting in pedestrian environment (almost exclusively on Mexico border). It's hard to take pictures of moving cars. We think there's value to doing air, have to start somewhere.
- BG: Privacy compliance framework for Traveler Verification Service (TVS)
  - List of relevant PIAs
  - Program comes to us early and often.
  - Making sure there's signage and tear-sheets available.
  - Working with PRIV and advocacy committee.

- o We'd like a collaborative relationship with DPIAC as well.
- o Q (Robyn Greene): what privacy protections are you using? Are protections the same across populations?
    - ▪ A(MH): currently yes.
    - ▪ Q(RG): is it shared with other offices?
        - • A(MH): cautious no. We might share information with NIST to analyze accuracy.
        - • A(BG): we must distinguish because photos themselves (14 days) and the exit records itself, which could be a routine use.
    - ▪ Q(RG): mission creep worries?
        - • A(MH): I struggle with the slippery slope argument; as a fed employee I should be held accountable to what we're doing, but not for all hypothetical situations.
    - ▪ Q(RG): Jet Blue pilot—are they in control with the photos? Limitations of use?
        - • A(MH): we have an MOU with them. They've agreed to our terms, and have also stated their business model doesn't benefit from the retention of photos.
- o Q (Joanne McNabb): I assume this is covered in the PIAs?
    - ▪ A(MH): yes.

2:35 p.m. Tasking – Facial Recognition

Lindsay Lennon Vogel (Senior Director, Privacy Compliance (Acting), Privacy Office, DHS)

- • Reading briefing.
- • Please consider applicability to other parts of DHS.

- • Lisa Sotto: Joanne McNabb is leading the tasking.

- • Joanne McNabb: the question is broad, but focused on CBP. So you want broad recommendations?
    - o LVL: speak specifically on CBP, but we'd like broad recommendations in our pocket.

2:40 p.m. Break Please return by 2:50 p.m.

2:50 p.m. - 3:15 p.m.

Immigration Data Initiative

Marc R. Rosenblum (Deputy Assistant Secretary, Office of Immigration Statistics, Office of Policy, DHS)

- • Michelle: ESC to give DHS Stakeholders real/near-real-time information
- • Overview of structure of ESC

- Had to get a One DHS exception because law enforcement components shouldn't be getting this information
- History: DHS systems are largely case management systems; OIS asked to generate aggregate statistics
  - So, do we have the same records moving across systems?
- Describing phases of project.
- Trying to move from manual transfer (encrypted CD) to electronic transfer
  - Direct access to database, set up FTP
- Challenges
  - Per executive order, some of the annual reports now are quarterly/monthly
  - Establish data sharing policies
  - Phase 3 is part of the reason why we're here today
- Outcomes slide
  - Use cases
    - TSA has approached them for help
    - ICE has had to reenter data because transfers between systems don't work
  - JRC documents/processes
    - Trying to stay system agnostic—heading towards Data Framework
- Q (Sharon A.): What do you mean by "Data Framework"?
  - A(M): DF is the name of a DHS system. We're providing data quality, but they're handling privacy/CRCL concerns.
- Q (Jim Adler): we had done a bunch of work on Cerberus, etc., has that become DF?
  - A(M): yes.
- Enforcement lifecycle slide
  - Not all statisticians are experts on underlying policies, but quality of data for reporting depends on knowing the differences.
- Disclaimers Slide
- Enforcement Lifecycle Slide
- Screenshots
  - First one shows you 70% removal within a year
  - Second one shows you where the rest are and what status they have
- EOIR slide
  - Explanation of One DHS exception
  - Q(Lisa Sotto): what's EOIR
    - A(M): Executive Office of Immigration Review
- Q (Jeff Brueggemann): any re-identification risks?
  - A(M): there are some risks; that's one of the questions we have.

3:20 p.m. Tasking – Best Practices for Protecting Immigration Statistics Data

Christa Jones (Senior Director, Privacy Policy and Oversight, Privacy Office, DHS)

- Lisa Sotto: Joanna Gramma will be leading it. Sharon will confer with Joanna. Note: we did a paper a few years ago that may be relevant.
- Christa Jones:
    - IDII has both operational and statistical uses
    - Tasking focuses on "behind the door"
    - Reading briefing
- Q (Sharon A.): are you looking at this because of best practices or because you think it's required by regulation?
    - A(M): we want to be able to report as req., but want to be careful to not reveal too much (like unaccompanied children).
- Q (Debbie M): will it be statistical data or deidentified microdata?
    - A(M): both depending on stakeholder.
- Q (Peter Sand): what is the scope of your inquiry? Anonymized enough just based on this data, or if in context of all data available?
    - A(M):
    - A(CJ): maybe on a practical level, we can't publicly release any microdata.
- Q (J.A.): relationship with Data Framework?
    - A(M): we think we will go that wall, but unclassified side has been much more complicated for Data Framework than classified.

3:25 p.m. Public Comments

- Harrison Rudolph, GULC CTP
    - CBP has not provided a good reason to collect American biometrics.
    - Congress wanted foreign nationals, CBP chose to collect Americans.
    - Notice doesn't reflect ability to opt out.
    - CBP's 96% benchmark doesn't account for people flying under false identities, which means that doesn't actually tell us how effective it is.
    - CBP has told us today that they are studying effects of disparate racial impact, that study should be publicly released.
    - CBP has not properly done NPRM.