Transcript of Public Meeting

Tuesday, February 22, 2022

Meeting of the Data Privacy and Integrity Advisory Committee
U.S. DEPARTMENT OF HOMELAND SECURITY

MEETING OF THE DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

Virtual Meeting

10:30 a.m.

Tuesday, February 22, 2022

U.S. Department of Homeland Security

2701 Martin Luther King, Jr., SE, Mail Stop 0655

Washington, DC 20598-0655
Ms. Taylor: Good morning, everyone.

Good morning. So we will be starting momentarily. Our members are just coming in. Welcome to the public meeting of the Data Privacy and Integrity Advisory Committee.

We are going to start in a couple of minutes, but we can give our members an opportunity to join us. Please keep your mics muted until you are speaking, and that will be done during the question and answer session. Our members are coming in. And thank you all very much.

Thank you for your patience. We want to give it a couple more seconds or minutes, and then we are going to get started. Alright. Okay, good morning. It is now 10:32 a.m., and this meeting is called to order. This is the public meeting of the Data Privacy and Integrity Advisory Committee, better known as the DPIAC.

Again, welcome. We have committee members and members of the public joining us today. If you have any difficulties hearing or seeing at any time, please let us know. And please remember again to mute your mics until it is time for Q&A or public comment session -- session, sorry.

The media agenda and the materials for today's session can be found on the DPIAC's website. And I will put that in a chat soon, so you will see it. I will now take a quick roll call before I turn it over to the committee chairperson, Lisa Sotto for opening remarks. So with that, I am going to start calling on members. Please just respond present. Sharon Anolik?

Ms. Anolik: Present.

Ms. Taylor: Courtney Barton?

Ms. Barton: Present.

Ms. Taylor: Dennis Dayman?

Mr. Dayman: Present.

Ms. Taylor: Michael Fitzpatrick?

Mr. Fitzpatrick: Present.

Ms. Taylor: Mark Francis?

Mr. Francis: Present.

Ms. Taylor: Joseph Hewitt?

Mr. Hewitt: Present.

Ms. Taylor: Sarah Knight? Sarah Knight?

We still have people coming in.

Ms. Knight: Present.

Ms. Taylor: Thank you, Sarah. John Kropf?

Mr. Kropf: Present.

Ms. Taylor: Rosal Marshall?


Ms. Taylor: Ade Odutola?

Mr. Odutola: Present.

Ms. Taylor: Chris Pahl?

Mr. Pahl: Present.

Ms. Taylor: Charles Palmer?

Mr. Palmer: Present.

Ms. Taylor: Harriet Pearson?

Ms. Pearson: Present.

Ms. Taylor: Tom Plofchan?

Mr. Plofchan: Present.

Ms. Taylor: Sasha Romanosky?

Mr. Romanosky: Present.

Ms. Taylor: Cameron Russell?

Mr. Russell: Present.
Ms. Taylor: Thomas Siu?
Mr. Siu: Present.
Ms. Taylor: Chairperson, Lisa Sotto?
Ms. Sotto: Good morning.
Ms. Taylor: Chris Teitzel?
Mr. Teitzel: Present.
Ms. Taylor: Great. Ray Thomas? Ray Thomas?
(No response.)
Ms. Taylor: Surbhi Tugnawat? Surbhi?
(No response.)
Ms. Taylor: Ron Whitworth?
Mr. Whitworth: Present. Good morning.
Ms. Taylor: Good morning. Thank you again for joining us today. And now I turn it over to our committee Chairperson, Lisa Sotto.
Ms. Sotto: Alright. Thank you so much, Sandy, and thank you all for joining us today.
Good morning and welcome to this meeting of the Data Privacy and Integrity Advisory Committee.
Before we begin, just a couple of housekeeping matters. If I could remind everyone to please mute your mics for the duration of the presentations.
There is designated time for committee member questions after each presentation. And there is also designated time for public comments at the end of the session today.
For members of the public who would like to address the committee during the public comment portion of the session, we ask that you please email privacycommittee@hq.dhs.gov. I am going to repeat that, privacycommittee, all one word, privacycommittee@hq.dhs.gov.
So welcome to returning and to new committee members. Chief Privacy Officer Lynn Parker Dupree and members of the public will join us hopefully today. Don't know yet about public comments, but certainly we will have some good presentations.
To help us facilitate questions and comments after each presentation, committee members should use the chat function to indicate that they wish to speak. For those of you who have not been to a live meeting, we typically use tent cards and we put them upright to indicate a desire to speak, but we are going to have to do it a different way for now, and hopefully we will be meeting live soon enough.
So there will be time at the end, as I said, for public comments and just send an email to that email address. Again, privacycommittee@hq.dhs.gov, if you would like to submit -- if you would like to ask a question as a member of the public.
We have a terrific agenda today. Chief Privacy Officer and Chief Freedom of Information Act Officer Lynn Parker Dupree will provide the committee with an update of the Privacy Office's activities. And following her presentation, we are going to receive updates from the Policy and Emerging Technology subcommittees on their testing progress.
There will be time for committee member Q&A after each subcommittee briefing. And as a reminder, the tasking information is available on the DPIAC web page under meeting information for October 27th, 2020. That is when we got those taskings. Following these discussions, we have reserved time for public comment beginning tentatively at 11:50 a.m.
We have not received advance notice from anyone wishing to address the committee, so we will open the floor to members of the public at that time. But please keep in mind that we may open the public comment period early if presentations run short. So if you have a question, please keep that in mind.
Again, please mute your phones and your computers, if you are not presenting or speaking or asking questions during any Q&A period. And now, I will turn it over to Chief Privacy Officer Lynn Parker Dupree. Thank you, Lynn.
Ms. Dupree: Thank you so much. Good morning, everyone, and thank you for joining today's public meeting of the DPIAC. I am very excited to be able to meet with the committee again and provide updates on the Privacy Office's activities and hear updates related to your ongoing
work on behalf of the Department. I am also incredibly excited to congratulate our new and returning members on their appointments to the DPIAC.

I greatly, greatly value the DPIAC's contributions to the Department's work in protecting privacy, and I see the selection of our members as an important part of my goal in improving the Privacy Office's engagement with our important stakeholders. To get us started, I am going to give you an update on some of the Privacy Office's most notable achievements over the last year, as well as one of my priorities moving forward.

I am approaching my one year anniversary as the DHS Chief Privacy Officer, and I am very proud of what we have been able to accomplish and look forward to building on those achievements. As I noted earlier, I am really committed to improving the Privacy Office's engagement with our stakeholders.

So in addition to revitalizing the DPIAC, we have rebuilt our relationship with our external privacy advocates and brought a diversity of opinions to the Department's policy discussions through those external engagements. This included arranging an opportunity for privacy advocates to discuss their priorities directly with Secretary Mayorkas.

I have also held several other meetings with privacy advocates and DHS leaders to better understand their positions regarding critical DHS activities, like our efforts to combat domestic violent extremism and other important operations that intimately impact the public.

And while our stakeholders positions may not always be aligned with that of the Department, these discussions ensure that a diversity of opinions are included in our thinking and really help improve our decision making. I also focused on strengthening the Privacy Office's relationship with the component Privacy Officers as well as other Federal agencies.

So I regularly meet with component privacy officials to ensure that the Headquarters Privacy Office is aware of any evolving issues and to provide assistance when necessary. I have also been proud to highlight DHS's approach to privacy as a speaker at many events, including the intelligence community's Privacy and Civil Liberties Summit, events hosted by the International Association of Privacy Professionals, the Federal Privacy Summit hosted by the Federal Privacy Council, as well as others.

Over the last year, the Privacy Office has also helped to shape the Department's response to a number of activities that have significant privacy implications, such as ensuring our community and workforce health during the pandemic, again, responding to domestic -- to domestic violent extremism, and focusing on the use of emerging technologies.

As many of you may know, the Privacy Office basically identifies and we address our privacy risks through our privacy compliance documentation process, and the secretary has sent a clear message about the importance of including the Privacy Office in these policy discussions.

Additionally, I have really tried to spend some time embedding resiliency into the Privacy Office's operations. So in addition to developing a culture that supports and values promoting training and expanding the professional development of the staff, I also supported the engagement of the Chief Financial Officers Program Analysis and Evaluation Office to develop and create a staffing allocation model, and this model accounts for all of the office's workflows and helps us plan to better meet our work demands.

We have also brought on several new members to the Privacy Office staff, and we are working on several other hiring actions to increase resiliency. And before I move on to the Privacy Officer's priorities for the next year, I do want to recognize my dual role as the Chief Privacy Officer and the Chief FOIA Officer and share some exciting news about DHS FOIA operations.

The Department ended the last fiscal year
with the lowest backlog in almost a decade. In achieving this milestone, we processed a record number of -- a record breaking number of requests. And I am particularly proud of the way that we used our FOIA resources in the Privacy Office, not only to handle our own workload, but to also help other components close out many of their requests.

Now, I would like to move on to some Privacy Office priorities for Fiscal Year 2022. One of my top priorities is to shift privacy implementation from being solely focused on governance, which is extremely important and remains to be invaluable, but to also include privacy in the technical design.

The Privacy Office is working with DHS stakeholders to host a workshop in June of 2022 that will enable privacy researchers to identify DHS use cases that could be solved with privacy enhancing technologies. And then what we can do is then connect that -- those discoveries with the program offices so that they can be used in building out our programs and our operations.

Now, I understand that these research initiatives are not going to happen overnight, but it is something we need to start thinking about now and seek over the long haul if we are going to ensure that Privacy Office moves into the future and that we are able to respond proactively instead of reactively. Another priority I have for Fiscal Year 2022 is the expansion of the tool we use to track our privacy compliance documentation and that tool is called PRIVCATS.

And we are exploring how we can use this tool to help the Privacy Office in its other requirements and functions, including our congressional reporting, including responding to the recommendations from OIG or from GAO. I see this as a -- this update as a valued opportunity to embed technology assisted documentation of the Department's programs and the systems in our processes, and it will allow the Department to gather necessary information from the programs and then store that in a centralized location.

And finally, I am focused on the launch of the new DHS FOIA processing solution. It is called Secure Release. And Secure Release will help us meet the demands of a modern FOIA program and provide us with the tools we need to serve the Department and the public. It will enable us to reduce the number of FOIA processing systems that exist across the Department and will help us ensure that any system that is in use is interoperable and improve the consistency of our redactions across components.

And to the committee members, I want to thank you all for your time and your dedication, and I am really looking forward to leveraging your expertise to provide tangible and achievable recommendations to the Department. I am very excited to have the opportunity to work with you all. Thank you.

Ms. Sotto: Do we have any questions? Committee members -- okay, I don't see any hands raised. Thank you so much. We really appreciate the update, and I will say that I think there is great enthusiasm for revitalizing the committee and helping you do your work and helping the Privacy Office generally. So please, please, please use us as you wish. We are here and we are here to help.

So thank you so much. There was a terrific update, and we appreciate it.

Alright. So now it is time for a briefing from the DPIAC Policy Subcommittee Chair Dennis Dayman. Mr. Dayman is going to provide the committee with an update on the information sharing tasking. So, Dennis, let me turn it over to you.

Mr. Dayman: Thank you, Lisa. I appreciate that. Hello, everyone. Welcome. I am glad to see that we are all back here. Yes, what we wanted to do today was to kind of give you an idea of where we are with our tasking.

As you are aware, and I will kind of review this very quickly, is that the DPIAC was tasked with providing recommendations obviously to the Privacy Office on how to better oversee information sharing across the Department of Homeland Security offices and components.

This tasking, as Lisa has mentioned,
began on October 27th of 2020, when they asked DPIAC to provide guidance and information sharing specifically on a couple of different points. They -- it was asked to have written guidance on best practices, again, to ensure the effective implementation of privacy requirements for information sharing within the DHS enterprise.

And at the time, the Privacy Office asked that, how can DHS Privacy Office better engage with their own offices and components to improve consistency in meeting information sharing requirements that are related to privacy? Number two, how can the DHS Privacy Office provide better oversight of privacy protections included in information sharing agreements? And were there any sort of specific metrics that can be utilized and written in those agreements to make sure that there is compliance within those?

And then third, were there any other considerations necessary to effectively implement privacy requirements to DHS sharing information? Again, this tasking was assigned to the policy subcommittee, and I myself along with committee members spent a great amount of time meeting over the last year or so, not only with ourselves and staff being a part of that, but also taking the time to look at several different processes, but also a lot of document requests into DHS staff so that we could sort of see what the -- what we needed to understand.

As a very quick sort of key example is in those documents. We looked at everything from the Office of Inspector General's report that came out in November of 2020 and several other management directives and policy directives that we felt would help us understand the processes within DHS, and again its partners, in handling privacy and managing it, monitoring it, and then continually looking at it every couple of years. Again, you know, spending a lot of time, you know, with the committee, we basically made some recommendations so far in this report.

This report has actually been submitted over for review. It was submitted in November of last year, but when we sort of take a look at it from very high level, the report reflects a detailed review by the committee of the current status of information sharing practices and provides what we think are recommendations that would help promote consistency in baseline privacy controls for those information sharing and then facilitate oversight by the Privacy Office across all, again, those information sharing activities, and really to achieve better engagement across the DHS offices and its components.

Very quickly, just on a high level, again, some of the things that we are looking at doing was looking at adopting template information sharing and access agreements known as ISAAs, and privacy addendums that can be included in existing and future sharing agreements that would involve PII or personal identifiable information, and other things as well.

With these core capabilities in place, we believe that the Privacy Office will be able to engage, again, with its appropriate stakeholders across the offices within DHS and components to provide even things like training and awareness, leading to increased adoption and compliance when it comes to privacy.

I am trying to think here -- really at this point, like I said, we have submitted the report over to the staff and to the committee in November, and we are looking forward to actually bringing this to the much higher DPIAC committee for discussion and for input as well.

So Lisa, I will turn it back over to you then.

Ms. Sotto: Okay, I am going to ask for questions. Any questions at all? No member questions for Dennis.

Mr. Plofchan: Lisa, just a quick one.

Do we have a timeline on that larger conversation with the greater committee?

Ms. Taylor: Hey, this is Sandy. Lisa, I am happy to jump in --

Ms. Sotto: Yes, please.

Ms. Taylor: Thank you so much. So as
you know, we actually had to wait until we had new members seated.

And now that that is done, I am going to have a conversation with the Chief -- with Lynn Parker Dupree, the Chief Privacy Officer, and we will come up with a time when we can have another public meeting, possibly within the next two months, so the committee can vote on these recommendations.

Mr. Plofchan: Excellent. Thank you.

Ms. Taylor: You are welcome, Tom.

Thanks, Lisa.

Ms. Sotto: Okay. Any other questions?

I don't see any hands raised or feel free, if you are committee member, to jump right in. Okay. And just a reminder that we will take public comments at the end of today's session.

So if there are no more questions for Subcommittee Chair Dayman, I will turn it over now to the Emerging Technologies Subcommittee Chairperson Chris Teitzel for an update on that committee's tasking. Chris, over to you.

Mr. Teitzel: Thanks, Lisa. So the subcommittee met several times over the last year and a half to discuss a tasking also from the 27th, same time that the policy subcommittee also had their tasking. Ours was a bit interesting of a tasking because it was a tasking to find a tasking.

The tasking itself was to consider the Department's transition to cloud service technologies and enhanced capabilities that the transition provided during the Department's COVID-19 telework, you know, migration that they underwent at the beginning of the pandemic.

As an overview, the Department saw a 7x increase in the number of Tesla workers, a 200 percent increase in traffic, and the VPN usage increased by 483 percent. So a massive shift, as we all did during the pandemic, to remote work and telework.

And the consideration was, what does -- what impact does that have on data, and not only the privacy of the data, but the integrity as various systems during that telework migration were also being moved to cloud environments as well, and that had been happening for quite a while. Luckily for the Department, during the winter, snowstorm of 2018, 2019, a large shift had already occurred during that time, so much of the rough spots were found and attended to during that transition in 2018, 2019.

And so from that, you know, the transition actually went very smooth. So the committee met with the Office of the Chief Information Officer, the OCIO, office and representatives there. Now, we got briefings on cloud systems that were currently migrated, going to be migrated, and ones that were tagged for not to be migrated and to stay in localized data centers.

We went through with those individuals and then we had discussions internally on the various risks of what cloud migration entails, how data moving from one source to the other can then be exposed, and how to take certain precautions around that. We found that because this was a tasking -- for a tasking, there wasn't as much follow on that needed to happen.

And so we put all that together into a report. That report has been passed over to the Privacy Office, and now we are working with Sandra and others to, like I have mentioned earlier, we will be scheduling the meeting for a larger discussion with the group as well.

And so at this time, the report is written and ready to go, though as we bring on new members, I am sure there is going to be new input that we will likely get, and we are looking forward to having it.

And so, you know, before that meeting, it would be great to have any new members of the Emerging Technology Subcommittee take a review of that and offer any advice as well.

Ms. Sotto: Thank you so much, Chris. Is there anyone on the committee who would like to ask the question of Chris? And I will remind committee members, please, to email Sandy, you can certainly copy me if you like, with your selection for the
1 Policy Committee or the Technology Policy
2 Subcommittee or the Technology Subcommittee.
3
4 We would love to be able to get as many
5 people their choice of subcommittee as we can. And
6 so please let us know. Anything else from the
7 committee? Okay. If there are no more questions
8 for Subcommittee Chair Teitzel, I will turn it over
9 now to Chief Privacy Officer Lynn Parker Dupree to
10 issue a new committee tasking.
11
12 Ms. Dupree: Thank you. This tasking is
13 focused on the Department's use of commercial data
14 and will be the third time the DPIAC examines this
15 topic.
16
17 The DPIAC first analyzed the Department's
18 use of commercial data in 2005 and was focused on
19 the Department -- how the Department might use
20 commercial data to reduce false positives in its
21 screening programs and outline controls to help
22 protect privacy in those circumstances. The DPIAC
23 issued a subsequent report in 2006, which built on
24 the work conducted in 2005 and made additional
25 recommendations.
26
27 Some of those recommendations were
28 definitional and others provided insights on how to
29 leverage our compliance documentation process to
30 analyze commercial data use. Since 2006, the DPIAC
31 has not produced any additional recommendations
32 related to commercial data.
33
34 In the interim, the sources and uses of
35 commercial data have both advanced and expanded.
36 To that end, I am tasking the DPIAC to build upon
37 the previous reports to provide their views and
38 recommendations on a governance policy and
39 framework wedded to the use of commercial data and
40 DHS programs.
41
42 I eagerly await your recommendations and
43 analysis.
44
45 Ms. Sotto: Thank you very much. We
46 appreciate that, and we are eagerly looking forward
47 to diving in. Sandy, could I ask that you please
48 send to committee members the prior reports, the
49 2005 and 2006 reports on the use of commercial
50 data?
51
52 Ms. Taylor: I will. Lisa, along with
53
54 that, the new tasking. And also just for our
55 members of the public, this new tasking will be
56 made available immediately following this meeting
57 on the DPIAC's website.
58
59 Ms. Sotto: Okay. That is perfect.
60
61 Thank you so much. And as I said, we are eager to
to dove in, so we will do so and then organize which
62 subcommittee will be taking this particular
63 tasking. Okay. Are there any questions for Lynn
64 before we move on?
65
66 (No response.)
67
68 Ms. Sotto: Okay. And that was questions
69 from the committee. Okay. So let's go ahead and
70 move on. Sandy, I am not aware that anybody has
71 pre-registered. Has anything come in?
72
73 Ms. Taylor: No. So we do not have
74 anyone who pre-registered for public comment.
75
76 However, we can open it up at this time for any
77 member of the public who has a question either for
78 our Chief Privacy Officer or our members. Okay, I
79 see that Mr. Myerson has a question.
80
81 Mr. Myerson: Yes, hello. Good morning.
82
83 I did pre-register in that requested comment, so I
84 thank you for giving me the floor. Hi, my name is
85 Ted Myerson. I am the President and Co-founder of
86 Anonos. And Anonos applauds the DHS's focus on
87 reviewing advanced PTs in the age -- the rapid age
88 of digital transformation. There is not one
89 solution that solves every use case.
90
91 However, we recommend that the DHS
92 research the benefits of dynamic pseudonymization
93 technology. As recently recognized by the World
94 Economic Forum, the European Data Protection
95 Supervisor known as the EDPS, and the European Data
96 Protection Board known as the EDPB, as really one
97 of the most cutting edge tools to eliminate
98 unnecessary tradeoffs between data privacy and
99 utility.
100
101 It is really one of the most advanced
102 forms of data protection by design by default, and
103 we believe it is one of the DHS's top priorities to
104 evaluate technology that is more than just by
105 design, but rather is implemented at the earliest
106 possible point by default.
So just as the use is dynamic in today's world, effective data protection must be dynamic to protect data when it is in use so it can travel safely beyond companies and Government offices perimeters, for protected processing in the cloud and sharing, and combining among partners and organizations.

And just for some brief background, the European data privacy regulators, the EDPB and the EDPS, have highlighted pseudonymizations as the only solution to lawfully transfer data internationally and lawfully process EU data and the U.S. operated clouds.

And the World Economic Forum just highlighted pseudonymization as a fourth industrial revolution technology capable of resolving these conflicts between data use and protection. So as dynamic pseudonymization technology enables surveillance proof processing while maintaining maximum utility and 100 percent accuracy of the data when compared to processing in unprotected clear text.

And so some of these benefits, they don't require the heavy processing and transmission, such as homomorphic encryption or multi-party computing that can be used in some of these most advanced analytics, such as like AI, ML, without compromising speed, utility, or accuracy. And this also defeats the unauthorized linking to identity known as the mosaic effect.

So to conclude here, any long term sustainable approach to balancing data privacy, protection, and national security should include dynamic pseudonymization that satisfies the highlighted and heightened requirements and delivering the significant benefits recently highlighted by the EDPS, the EDPB, and the World Economic Forum. Thank you.

Ms. Sotto: Thank you very much, Mr. Phillips. Any other questions from members of the public?

(No response.)

Ms. Sotto: Okay. If there is anything else that -- please do feel free to submit written comments. You can submit them to the same email address, it is privacycommittee@hq.dhs.gov. We ask that you please submit those by March 3rd, with respect to written comments that are specific to this meeting.

Please keep in mind that we operate as a Federal advisory committee under the Federal Advisory Committee Act, so all written comments are treated as public documents and will be available for public inspection.

And with that, many thanks to Chief Privacy Officer Lynn Parker Dupree, committee members, and members of the public for participating in today's meeting.

This concludes today's meeting. We are grateful for your interest. We encourage you to...
follow the committee's work by checking our web page, and the minutes of today's meeting will be posted there in the near future.

With that, this meeting is adjourned.

Thank you.

(Whereupon, at 11:05 a.m., the meeting was adjourned.)
< W >
wait 22:1
want 3:13 13:18 16:11
wanted 17:14
Washington 1:22
way 8:2 14:4
web 8:22 34:1
website 4:6 28:4
wedded 27:12
Welcome 3:4 20 6:19
7:12 17:12 22:11
well 10:13 11:20 12:10
20:19 21:10 24:1 25:8, 17
went 24:9, 17
Whitworth 6:12, 13
winter 24:3
wish 7:21 17:3
wishing 9:6
word 7:10
work 10:1, 6 13:13
16:16 17:1 23:17 26:21
32:14 34:1
workers 23:14
workflows 13:12
workforce 12:15
working 13:16 14:15
25:5
workload 14:6
workshop 14:16
World 29:10 30:2, 14
31:15
written 18:4, 17 25:10
33:6, 10, 14

< Y >
year 10:13, 15 12:11
13:18, 22 14:9 15:8
19:3 20:1 23:2
years 19:17