

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

DEPARTMENT OF HOMELAND SECURITY
MEETING OF THE
DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

Wednesday, November 7, 2012

Room B 1.5-10
Ronald Reagan Building
1300 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

The transcribed portion of the meeting was
convened, pursuant to notice, at 2:50 p.m., LISA J.
SOTTO, Chairman, presiding.

1 ATTENDANCE

2 COMMITTEE MEMBERS PRESENT:

3 Lisa J. Sotto, Chairman

4 Craig Bennett

5 James M. Byrne

6 Renard Francois

7 Melodi M. Gates

8 Joanna Grama

9 David A. Hoffman

10 Greg Nojeim

11 Charles Palmer

12 Christopher Pierson

13 Tracy Ann Pulito-Michalek

14 Barry Steinhardt

15 Marjorie S. Weinberger

16

17 ALSO PRESENT:

18 Dan Chenok, Chairman, Cybersecurity Subcommittee

19 Sharon Bradford Franklin, Member, Cybersecurity

20 Subcommittee

21

22

1 P R O C E E D I N G S

2 MS. SOTTO: All right, folks. Let's
3 proceed and move ahead. We are going to now welcome
4 the Cybersecurity Subcommittee to take the floor.

5 In December 2011, the committee was asked
6 to research what privacy considerations DHS should
7 include in evaluating the effectiveness of
8 cybersecurity pilots. We were also asked to
9 research what specific privacy protections DHS
10 should consider when sharing information from a
11 cybersecurity pilot project with other agencies.

12 We are delighted to welcome Dan Chenok who
13 is the chair of the Cybersecurity Subcommittee,
14 which is composed of both -- and this is unusual for
15 us -- DPIAC members and non-DPIAC subject-matter
16 experts who were brought in to help with this
17 particular topic. These are folks who have
18 appropriate security clearances and have received
19 several substantive briefings on DHS cybersecurity
20 activities to help inform their research.

21 We are deeply grateful for those of you
22 who were not on the committee, especially -- and of

1 course, those of you who are -- for contributing to
2 this very important topic. I think it's so critical
3 to understand that these contributions will help the
4 Privacy Office and will help DHS in embedding
5 protective practices going forward.

6 I would note that a few non-subcommittee
7 members also have looked at the paper. I have.
8 Howard Beales has and Charles Palmer, who has
9 stepped out for a bit -- have looked at the paper in
10 advance and have provided comments. So we're very
11 grateful to Charles and to Howard as well for their
12 help.

13 With that, I'm going to turn the floor
14 over to Dan to provide some color as to the paper.
15 Hopefully, you've all had a chance to read it and
16 have comments at the ready and questions, and Dan
17 and Sharon and others can respond.

18 The goal today, if we can get there, is to
19 go ahead and formally adopt the report as a
20 committee issuance. With that, Dan, thank you very
21 much.

22 MR. CHENOK: Thank you, Lisa. I assume I

1 should wait for Shannon to deliver on the phone.

2 Thank you, Shannon.

3 Thanks again, Lisa, and thanks to the
4 DPIAC for having us here today. As Lisa said, I'm
5 Dan Chenok. I'm the, I guess, de facto chair of the
6 subcommittee.

7 The subcommittee came together actually a
8 couple years ago after the White House 60-day
9 cybersecurity review, which some of you may
10 remember, and there was a recommendation from that
11 review that DHS assemble a group of privacy experts
12 and provide them, as Lisa said, with clearances so
13 they could have discussions with DHS like the
14 discussions that Brendan described earlier around
15 cybersecurity programs and pilots and the privacy
16 considerations in that. And through the course of
17 the committee's work, we then basically under the
18 leadership of Mary Ellen Callahan, the then CPO,
19 became affiliated as an ad hoc committee of the
20 DPIAC. And I do want to acknowledge, in addition to
21 Sharon who is on the committee, the other members of
22 the subcommittee, two of whom are here, Chris

1 Pierson and David Hoffman, who are part of this work
2 that we'll be talking to you about; two others who
3 are on your committee, Joanne McNabb and Linda
4 Koontz; three who were on your committee, Richard
5 Purcell, Ramon Barquin, and Lance Hoffman; and then
6 other subject-matter experts known to, I'm sure,
7 some of you, Steve Bellovin, Fred Cate, and Mort
8 Halperin. And so together, that's the group that
9 basically represented input into the product that
10 we'll talk about today.

11 Just a very brief note, for those of you
12 that don't know my background, I chair a sister FACA
13 committee to yours. Under FSMA, there's a committee
14 called the Information Security and Privacy Advisory
15 Board, which advises NIST and OMB and the Congress
16 on such issues. So I chaired that board. I'm
17 actually outgoing after 6 years there. So I have
18 worked with a number of you in that capacity and am
19 happy to be here in this capacity now.

20 Basically the two questions that we were
21 asked in the letter that Mary Ellen sent to us in
22 December of 2011 that Lisa referred to were fairly

1 straightforward. One was what privacy
2 considerations should DHS consider when looking at
3 pilots involving the sharing of information. Some
4 of those questions, I know, came up in your
5 discussion earlier around the cyber pilot program
6 with Brendan Goode. And then what privacy
7 considerations should DHS consider when evaluating
8 the effectiveness of cybersecurity pilot programs.

9 So the subcommittee, having had numerous
10 discussions with one another and with DHS, both
11 Privacy Office staff, as well as staff from various
12 elements of the cybersecurity operation within DHS,
13 basically got together, reviewed our understanding
14 of those discussions, reviewed reports, including
15 the DPIAC's 2006 Privacy Analysis Framework, and
16 developed a set of recommendations that you received
17 a couple of weeks ago and that I will briefly walk
18 through for you today on the assumption that not
19 everybody has committed them to memory, and then we
20 can get into a discussion.

21 I will also add that thanks to Lisa and to
22 Howard and Charles for the very useful comments that

1 we received in the final drafting, many if not most
2 of which have been incorporated into the draft that
3 you received today. So we did welcome those and, of
4 course, will welcome your discussion after we have
5 the presentation for you.

6 First, just a reminder -- and I think
7 Brendan talked a lot about this, so we don't need to
8 spend a lot of time -- what is a cyber pilot, what's
9 the scope of the activity that DHS has to look at.
10 It's really the type of activity that you talked
11 about last hour. The Joint Cybersecurity Pilot
12 Program is an example where DHS worked with the
13 Defense Department around sharing information. The
14 EINSTEIN Program in its early stages, the pilot
15 initiative, is an example. And there are other such
16 examples. And I want to emphasize that the
17 recommendations we're making today are not related
18 to one particular cybersecurity pilot program but
19 are intended to be helpful with guidance for DHS in
20 thinking about cybersecurity pilots going forward
21 either now or in the future.

22 I will also emphasize that our scope

1 really does relate to those pilot programs as
2 opposed to other types of cybersecurity activities
3 that DHS is involved in that are sort of ongoing
4 programs. We really focused -- were asked to and
5 did focus on thinking about new programs, pilot
6 programs, where DHS is testing out new approaches to
7 cybersecurity, sharing information, et cetera.

8 So that's a general introduction. Was
9 there anything from the general frame that I missed?

10 MS. FRANKLIN: No.

11 MR. CHENOK: So let me go into a brief
12 discussion of our thoughts on the two questions we
13 were asked and then I'll ask my fellow subcommittee
14 members, starting with Sharon, to share any further
15 thoughts and then welcome your thoughts and
16 discussion as well.

17 Around the question about how to insert
18 privacy protections into the sharing of information
19 and pilot programs for that purpose, the first
20 finding that we made was that a principal goal for
21 any program involving sharing cybersecurity
22 information should be that the right information

1 reaches the right people at the right time. And
2 that means that you don't over-collect information,
3 you don't over-share information, really develop a
4 targeted program that looks at making sure that the
5 right level of information is collected. And we'll
6 get into some of the elements of what that looks
7 like around minimization and data retention and
8 that. But that was an overarching goal that we
9 thought was an important finding for these.

10 And the second and very important and I
11 think consistent with the work that's been done by
12 this committee is that the foundation for the
13 recommendations from a principles' perspective were
14 the DHS Fair Information Practice Principles, and we
15 felt very strongly that those principles had strong
16 applicability to cybersecurity pilot programs and we
17 wanted to start with that as a basis and didn't
18 really need to reinvent the wheel or think about
19 brand new approaches and frameworks. I think some
20 of the principles that we have -- you could probably
21 take those and tweak them in different ways but that
22 is the core element of where we started.

1 So a number of key recommendations for
2 pilot programs and sharing information: The first
3 is the subcommittee believed that it's important to
4 minimize, as much as possible, the amount of PII
5 that's part of any cybersecurity pilot. If
6 possible, don't use PII. If that's not possible,
7 minimize it; use it as least as possible.

8 The second finding was that if there is in
9 a cybersecurity pilot a piece of malware or a piece
10 of information that involves both identifying
11 information about the traffic, as well as
12 potentially content about the communications
13 underneath what that traffic looks like -- so
14 there's a piece of malware, and there's basically
15 maybe an e-mail or a document associated with that
16 malware -- that in order to really look beneath the
17 header information or the basic identifying
18 information of the traffic and into the content, the
19 pilot program should make a determination that the
20 risk posed by that activity is necessary and
21 necessitates a look underneath at the more detailed
22 information. And the subcommittee thought that was

1 an important distinction to make.

2 A third principle is around the Fair
3 Information Practice Principle of notice, that to
4 the maximum extent possible, DHS should notify the
5 public, other agencies, businesses about the nature
6 of the pilot program to the maximum extent feasible.

7 A fourth is that the sharing of
8 information should be limited where feasible to the
9 purpose of the pilot. So when DHS receives
10 cybersecurity information in a pilot program, the
11 sharing for that should be constrained within the
12 purpose of the pilot program for cybersecurity
13 purposes and that if there is a need to share beyond
14 that, there ought to be a strict set of rules around
15 what those look like. And I'll comment a little bit
16 on what those rules are before concluding thoughts
17 on the response to this question.

18 The first regards law enforcement. This
19 was a question that the subcommittee spent a lot of
20 time on in terms of internal discussion around when
21 should -- within information in a pilot program
22 should DHS share information with law enforcement

1 authorities, both within DHS and outside across to
2 the rest of the Federal Government and even state
3 and local governments. And basically you see in the
4 report some of the detailed discussion of this, but
5 the essential finding that we made, the essential
6 recommendation, is that sharing with law enforcement
7 should be limited in various ways to avoid the risk
8 of criminal prosecution without a sufficient
9 predicate. Sharon can expand on this a little bit
10 more because I think you have greater expertise in
11 this area. Do you want to go through that now?

12 MS. FRANKLIN: Do you want me to do that
13 now?

14 MR. CHENOK: Sure. That's great.

15 MS. FRANKLIN: The basic idea was to
16 distinguish between the real time on the ground --
17 the information is coming in and you need to act to
18 protect your networks -- versus being able to then
19 take data that is coming into DHS's hands for
20 cybersecurity purposes and then to go and start a
21 criminal investigation, and that if any criminal
22 investigation was to result, that there needed to be

1 a sufficient predicate to spell out what that would
2 be with exceptions for exigent circumstances and, of
3 course, complying with existing law, if there's a
4 warrant and so forth, but otherwise to make sure
5 that this isn't just a sucking up all sorts of data
6 that could then be used for unrelated criminal
7 prosecutions.

8 MR. CHENOK: We then took a look at
9 sharing with the national security community and a
10 similar finding, that information sharing should be
11 limited for purposes that are unrelated to
12 cybersecurity except where required by law, to
13 Sharon's point, or in exigent circumstances, and
14 that such sharing should basically have oversight
15 consistent with the Fair Information Practice
16 Principles, that the elements of notice and access,
17 et cetera, should apply to information that is
18 shared where feasible with the national security
19 community as well.

20 So we started with the law enforcement.
21 We took a look at national security. Then we took a
22 look at civilian agency sharing, and we said that

1 DHS as the lead for cybersecurity information in the
2 civilian space, consistent with the memorandum of
3 delegation of authority from the Office of
4 Management Budget under FSMA, should be the lead for
5 civilian agency pilots. And they are operating that
6 way now, and the subcommittee thought it was an
7 important element for pilots going forward in the
8 future.

9 We then took a look at sharing outside the
10 Government with the private sector. An important
11 finding that we thought was worth echoing here is
12 that the Government should not monitor as part of a
13 pilot private networks. The Government does do a
14 lot of sharing with private networks. You heard
15 some of that from the earlier discussion. But as
16 part of a pilot program, the subcommittee thought it
17 was important for the Government to encourage
18 companies, if they are providing cybersecurity
19 information to the Government, to where feasible not
20 include PII or the content of private
21 communications. To some extent that's not feasible
22 where a company may say look, we have a lot of

1 information. We just want to give it to you and in
2 that case, we thought it was an important
3 recommendation for DHS to delete where feasible or
4 as much as feasible PII or the content of private
5 communications from information that they do
6 receive.

7 So those were the four different
8 categories of sort of sharing that we looked at:
9 law enforcement, national security, civilian
10 agencies, and non-Government actors.

11 Finally, with regard to sharing, we took a
12 look at technology, and we know that technology can
13 be very helpful in terms of creating conditions for
14 protection of information so long as technology is
15 used properly to delve into the design of the pilot
16 program at the start. Things like randomization,
17 obfuscation, different types of technology
18 approaches we thought were important.

19 And then we lastly said that the
20 cybersecurity of the pilot program itself is an
21 important consideration in terms of privacy
22 protection. So it's a cybersecurity pilot program.

1 The program itself shouldn't have cybersecurity
2 problems such that PII or the content of private
3 communications is at risk or released unnecessarily
4 or in danger of harm.

5 Those were our principles around sharing.
6 Before I actually go to our principles for
7 evaluating, let me just ask if there's anything that
8 you wanted to add, Sharon?

9 MS. FRANKLIN: No.

10 MR. CHENOK: Chris, I'll come back to you
11 at the end if that's all right.

12 As far as the second question we were
13 asked -- actually in the letter it was actually the
14 first question, but we thought it was better to
15 share first and evaluate, better than evaluate
16 before you share. So we answered this question
17 second. We made a number of recommendations that
18 you can read about in summary.

19 The first thing we thought is that if you
20 actually look at the DHS documents for their
21 cybersecurity pilots thus far, at least at the time
22 that we looked at it, which was several months ago,

1 privacy itself was not an explicit evaluation
2 criteria for the success of the cyber pilots. And
3 we thought it was important -- because we knew DHS
4 was looking at this, we thought it was important to
5 make that explicit. So we made that a
6 recommendation.

7 The second is that groups like ourselves
8 were an important part of the process. As you heard
9 earlier from Brendan, he was appreciative of the
10 input from the subcommittee during the process of
11 the discussions that we had with them and we thought
12 that bringing in outside experts of various kinds
13 and, if necessary, clearing those experts and having
14 those kinds of discussions, in other cases having
15 discussions in public wherever possible because
16 transparency, we thought, was a very important
17 value, should be done as part of a cybersecurity
18 pilot.

19 Similarly, the Privacy Office and other
20 privacy expert elements within DHS and throughout
21 the Government should be involved in the design and
22 operation of the cyber pilot program from the

1 beginning. So the overall recommendation is use
2 expertise from the privacy community, both groups
3 like ourselves that are on the outside, as well as
4 privacy experts from the inside.

5 The third recommendation here was that
6 Privacy Impact Assessments should be done for each
7 pilot, done early. I would say done often, but that
8 would probably be redundant. But made public where
9 possible. The committee in the discussions with DHS
10 -- one of the things that we pointed out in the
11 report was that the public Privacy Impact Assessment
12 for EINSTEIN 2 -- or 3, the exercise initiative, was
13 a best practice in terms of disclosure, and we
14 thought that that was a model that could be
15 repeated.

16 An interesting finding and recommendation
17 that the subcommittee made regarding evaluations was
18 that if a cybersecurity pilot program isn't seen as
19 effective from the get-go -- in other words, you're
20 just kind of on an expedition to find something and
21 you don't know whether it's going to work -- that
22 there ought to be a reasonable expectation that the

1 pilot will work before you actually start it and
2 then start to collect privacy information of any
3 kind. So if a pilot program isn't expected to be
4 useful, it's not worth collecting PII at all, and we
5 thought that it was an important evaluation
6 construct to say that.

7 Another recommendation we made was
8 scalability. So we were, as we've talked about,
9 really looking only at the pilot program element.
10 But a clear evaluation criterion of any pilot is if
11 the pilot is found to be successful and you want to
12 scale it, will the same protections be feasible in
13 the scale model as they were in the pilot model?
14 And we thought that evaluating whether that
15 scalability was there present in the design and
16 likely to be successful in the future was an
17 important consideration.

18 With regard to oversight, an important
19 element of ongoing evaluation, we thought that
20 setting up an oversight process for cybersecurity
21 pilot programs was very important both for the
22 actual conduct of the program, as well as the

1 confidence of the users and the public that the
2 program is being done in a way that has good
3 governance. As part of that governance, we
4 recommended that the DHS Privacy Office be clearly
5 involved as a stakeholder and a leader in that
6 process.

7 We recommended that inspectors general
8 provide periodic audits, for example, every 2 years
9 of the program and its aftermath program.

10 And we recommended independent review,
11 wherever possible, by an independent entity with an
12 appropriate authority such as the Privacy and Civil
13 Liberties Oversight Board now that it's becoming
14 operational as we understand is happening. But
15 basically independent bodies like that with
16 appropriate authority we think are important
17 elements of the oversight process as well.

18 Our final recommendation around evaluation
19 was that the evaluation itself should also have a
20 high degree of transparency, that the questions that
21 DHS is asking, the findings that DHS is making, and
22 the reports are available for review and comment.

1 We ended the report with an appendix which
2 has a series of questions, basically a checklist if
3 you will, that take a lot of the recommendations
4 that we made and put them into a format that we hope
5 DHS would find useful in terms of actually
6 implementing some of these recommendations. The
7 questions are those that you might see as familiar.
8 They involve minimization. They involve retention
9 of information, making sure that the information is
10 not retained longer than necessary; involve access
11 of individuals to information about themselves;
12 redress, to the extent to which the pilot offers
13 redress opportunities; audit to make sure the
14 programs are being done properly; and oversight, as
15 I just mentioned, elements like that. And you can
16 see there are further questions in that list.

17 That was the report.

18 Let me ask Sharon if you have anything
19 else you wanted to add.

20 MS. FRANKLIN: I think you did a great job
21 in outlining.

22 I just want to emphasize a point that was

1 made at the outset. I know our subcommittee is
2 somewhat unique maybe in its structure, but I think
3 it has been very productive from my perspective. We
4 certainly heard that from the DHS folks. We have a
5 fairly broad range within the privacy experts. I
6 myself come from the NGO privacy advocacy community.
7 We have a lot of folks who work in corporate privacy
8 offices, academics. And so a range of perspectives
9 even on the privacy issues, and the DHS folks really
10 have been very engaged, very good reaching out to
11 us, and we've had some very good discussions. And
12 then in developing this paper, we've had some robust
13 debate among us on, you know, really parsing some of
14 these recommendations to try and make them ones that
15 we felt were good in terms of pushing privacy but
16 being, hopefully, helpful to DHS and within our
17 scope.

18 Also just to echo what Dan said. We put
19 in there -- not to pat ourselves on the back -- that
20 we recommend a committee like ours as a best
21 practice because we really did feel that has been a
22 productive dialogue along the way. So I just wanted

1 to echo that.

2 MR. CHENOK: Great.

3 Chris, do you want to add anything?

4 MR. PIERSON: Yes, absolutely.

5 It's kind of funny. You have different
6 people in front of you that come from all different
7 backgrounds and we all really gravitate towards of,
8 hey, this is the best practice.

9 Brendan -- his comments, the stuff he was
10 talking about today, his comments on the use, the
11 applicability, the values, the benefit of being able
12 to have this group be able to talk to, to question,
13 to listen to even just the group debate has been
14 extraordinarily beneficial for him in his role, as
15 well as good for the broader DHS community. I want
16 to kind of second and emphasize -- a third now I
17 guess -- and emphasize that that really is something
18 that is looking like it is a best practice. I hope
19 that that continues within DHS. I actually hope
20 that that extends outside of DHS, having folks that
21 come from legal backgrounds, from risk backgrounds,
22 from cybersecurity backgrounds, from privacy

1 backgrounds, folks with all different employers and
2 employer types be in the same room. That has been a
3 great benefit to DHS but also a great benefit in
4 terms of formulating thoughts as part of this
5 broader collective group.

6 Second -- it's however many pages we have
7 here -- 14 pages. This really was -- and there
8 really was a lot of discussion, a lot of review, a
9 lot of reviewing of older documents of older
10 meetings. There was a lot of thought and
11 forethought that went into this paper, and a lot of
12 it doesn't show it. There was a lot of debate that
13 was there, and I think that it was great to have
14 that discussion, to have that debate to really hash
15 out where things -- where we recommended things like
16 -- and I personally am proud to have been part of
17 that team.

18 I am proud with the work product that we
19 have produced, and I'm also proud that I believe
20 it's going to be something that can actually be
21 used. This has good guidance in it that will allow
22 the right decisions to be better made, to be better

1 understood. It's how this is used that is the most
2 important.

3 But I want to thank Dan for chairing all
4 of us through and shepherding us sometimes through
5 that process.

6 And maybe I'll turn it over to David.

7 MR. HOFFMAN: Just real quickly, once
8 again, I'd like to echo the thanks to Dan for
9 shepherding through and to everyone on the ad hoc
10 subcommittee for coming together really in good
11 faith from diverse perspectives to try to sort out
12 what would be the best way to analyze these issues.

13 I think the only thing I want to emphasize
14 -- it hasn't really been touched on -- is a bit
15 around the starting point that the subcommittee came
16 together around, which was an understanding that one
17 of the biggest risks to privacy that is out there in
18 the environment are security breaches that are
19 caused by bad cybersecurity. So this was a
20 particularly interesting project for many of us to
21 work on because we were working on making sure that
22 privacy was protected in the implementation of

1 cybersecurity programs which they themselves are at
2 least partially intended to also improve privacy,
3 which was one of the reasons why it was so
4 important, we thought, to first assess the adequacy
5 and the efficacy of the cybersecurity pilots and
6 that you see this multi-step process, that you by
7 providing utility from a cybersecurity pilot
8 implementation, you increase the ability to protect
9 private information when it's stored on networks
10 potentially, and then we move to the second step of
11 making sure that the way we implement those
12 cybersecurity measures actually does not have
13 unintended consequences of decreasing privacy in
14 other ways. And I really appreciated how the
15 committee came together to analyze those issues.

16 MS. SOTTO: Thank you very much to all of
17 you.

18 I'd like to now ask for questions and
19 comments from the broader committee. Marjorie?

20 MS. WEINBERGER: Kudos to all of you on
21 what I think is a tremendously beneficial paper for
22 operational purposes. By that I mean to steal from

1 it liberally in my own work.

2 (Laughter.)

3 MS. WEINBERGER: So thank you very much.

4 It does bring into account kind of next
5 steps, how do you make it happen and what are some
6 of the things you have to do to have in place so
7 that now you've got your commitments, you've got
8 conceptually the direction to go, because that's
9 what this is, a direction, really your road map to
10 get there. But you need other tools as well, and
11 I'm kind of hoping somehow these tools become part
12 and parcel of kind of your operational road map,
13 templates for agreements. You know, agreements are
14 going to be everything in this kind of thing because
15 there's a risk allocation, and with risk allocation
16 comes cost allocations. It's not going to come with
17 no risk and no cost, and how you determine how
18 that's done.

19 And when you deal with the Government, you
20 have the fun of indemnifications, which is, you
21 know, what does that really mean for Government?
22 And certainly Government can't indemnify private

1 parties which always becomes an interesting endeavor
2 when trying to contract with private parties because
3 they immediately want indemnification and you can't
4 constitutionally do it. I run into that on a daily
5 basis.

6 Also, in the worst case scenario, how do
7 you deal with damages? What is the role that the
8 parties will play in the worst case scenario so that
9 it's known up front? The idea is once you've
10 determined the allocation of risk, you also
11 determine allocation of cost associated with the
12 worst case scenario. So my hope is once you have
13 something like this, DHS will also come up with its
14 templates and suggestions of how to deal, you know,
15 once we've gone from conceptual into the real world,
16 of how do we make it happen and how do we protect
17 all of the actors as well.

18 MR. CHENOK: I think those are excellent
19 points, Marjorie. Thank you for sharing them.

20 On the question of tools and templates, I
21 couldn't agree more. We would hope that as David
22 and Chris pointed out, should we continue as an

1 entity, that DHS would like to discuss with us, we
2 would be happy to talk to you further about how you
3 can operationalize these, sort of the tools and
4 templates, how you can put it into a model PIA or
5 some sort of an automated tool for analysis, that
6 sort of thing. So we'd be happy to do that.

7 Sharon is my learned legal scholar here at
8 the table. I don't know if you want to talk about
9 indemnification or damages.

10 MS. FRANKLIN: That would be the
11 legislation. That would be what's going on in the
12 Senate. DHS has no authority to change the law on
13 its own.

14 MS. WEINBERGER: No, but it has to do with
15 how do you incent private companies to want to work
16 with you knowing you can't indemnify them. What can
17 you do? Because unless you come up with creative
18 language, they will always keep the door shut.

19 MR. CHENOK: We spoke a lot with DHS about
20 their information sharing programs and other
21 elements like that, and I think you're right. It's
22 just a challenge. It's a lot of blocking and

1 tackling in the absence of the legislation.

2 MS. SOTTO: Thank you.

3 Greg?

4 MR. NOJEIM: Great report.

5 One thought, comment. I think one concept
6 here is that if the pilot doesn't show that the
7 program will be effective, you don't go and fully
8 implement the program. But I'm not sure it came
9 through quite right in the document. I'm looking at
10 page 11 and the first bullet, the sentence beginning
11 "If a pilot." Is what you're trying to say there if
12 a pilot cannot establish a program's likely
13 effectiveness, then? Is that what you're trying to
14 say?

15 MS. SOTTO: Say that one more time, Greg.

16 MR. NOJEIM: If a pilot does not
17 effectively or cannot effectively establish the
18 likely effectiveness of a program. Is that what
19 you're trying to get to?

20 MS. FRANKLIN: The wording may benefit
21 from further wordsmithing. We had gotten a comment
22 from one of the full committee members who read this

1 to ask us to clarify this. The idea here is
2 separate from the point that you just made. The
3 point you just made is ultimately at the end if a
4 pilot runs and they say the program isn't going to
5 work, DHS shouldn't move forward with. That's a
6 separate point. What this is getting at is before
7 they even launch the pilot, if it doesn't look like
8 it can tell DHS anything, then it's not worth even
9 the potential privacy intrusion of the pilot itself.
10 This is supposed to be at the very beginning before
11 you launch the pilot, not at the end of the pilot,
12 to go forward with the program.

13 MR. NOJEIM: Two questions then. Why use
14 the words "assess the program's intended purpose"?
15 A pilot doesn't assess a purpose. Right?

16 MR. CHENOK: I would actually argue that a
17 pilot does assess a purpose. I think that there are
18 ways we can word it more effectively perhaps, that a
19 pilot -- when DHS sets up a pilot, it has a goal in
20 mind and then it basically says here's an activity
21 that you want to test to see if we can meet the goal
22 through a set of operational procedures. And

1 whether that's a purpose or a set of procedures or a
2 function, we can talk about which word to use.

3 MR. NOJEIM: I just thought it didn't come
4 through quite right.

5 A second question.

6 MS. SOTTO: A pilot is not effective in
7 facilitating the effective purpose, something like
8 that. Is that what you're saying, Greg?

9 MR. HOFFMAN: You're saying something
10 different. You're saying it's not about whether the
11 pilot is going to be successful itself or whether
12 the program is going to be successful. It's whether
13 the pilot serves the purpose of being able to
14 evaluate.

15 MR. CHENOK: It's whether it's a well
16 designed pilot.

17 MS. FRANKLIN: Whether it's a well
18 designed pilot that can, at the end of the pilot,
19 tell DHS what it needs to know.

20 MR. HOFFMAN: So it's not really assessing
21 the program's intended purpose but whether the
22 program will be beneficial.

1 MR. CHENOK: It's really where the pilot
2 can be beneficial.

3 MS. FRANKLIN: If a pilot cannot
4 effectively assess the program. Take out apostrophe
5 "s" and "intended purpose."

6 MR. CHENOK: That's fine.

7 MS. FRANKLIN: Take out the apostrophe "s"
8 and "intended purpose."

9 MR. NOJEIM: A second question raised by
10 your response to my first one is where in the
11 document does it say if the pilot shows a program
12 won't work, don't do the program.

13 MS. FRANKLIN: That may be the predicate.

14 MR. CHENOK: That's implicit in the entire
15 paper. We never make an explicit statement in that
16 regard. The closest thing we come is probably
17 scalability.

18 MR. NOJEIM: The concept I like was it's
19 not worth the privacy intrusion if it's not going to
20 work. So if you could capture that somewhere in
21 some language, I think that would be a useful thing
22 to have.

1 MS. SOTTO: How would you propose doing
2 that, Greg? Do you have any suggested wording?

3 MR. NOJEIM: I had suggested wording in
4 that other place, but let's see if there's another
5 place. Maybe in "oversight."

6 MR. HOFFMAN: Does the second bullet point
7 in that same section do what you're asking, Greg?
8 It says, "Once effectiveness has been established
9 and the program is deemed worthwhile." So if
10 effectiveness is not established, by inference the
11 program is not worthwhile.

12 MR. CHENOK: And you could expand and make
13 that a little bit clearer -- that clause.

14 MR. HOFFMAN: Right. So we could edit
15 that clause.

16 MR. NOJEIM: You could start that clause
17 with "if effectiveness has not been established,
18 then the program isn't worth any intrusion on
19 privacy rights and should be abandoned." Or add a
20 bullet.

21 MS. FRANKLIN: Add a bullet.

22 MR. NOJEIM: "If effectiveness has been

1 established, then." So the next bullet would read:
2 "If effectiveness has been established and the
3 program is deemed worthwhile, then."

4 MR. CHENOK: Okay. So I have that as "if
5 effectiveness has not been established and the
6 program is deemed not worthwhile, we recommend that
7 DHS not pursue the program."

8 MS. SOTTO: Or not pursue the collection
9 of personal information in connection with the
10 program.

11 MR. CHENOK: Good. Not collect PII or the
12 content of private communications as part of the
13 program.

14 Then the second parallel bullet would be
15 the one that we have now, which is if it is. Okay?
16 Good. Thank you.

17 MS. SOTTO: Further comments? Barry?

18 MR. STEINHARDT: Thank you. Excellent
19 report.

20 Here's my question. Much of the report
21 covers issues that relate simply to pilots. There
22 are some unique things, scalability, for example,

1 but it applies to any program along those lines. I
2 was wondering if you thought about -- I know it's
3 beyond your scope, beyond the scope of the question,
4 to go into this in detail, but I was wondering if
5 you thought about how to highlight those sections of
6 the report that also apply to programs that are
7 already operational or about to become operational
8 and pointing out that the same principles ought to
9 apply to those programs.

10 MR. CHENOK: So we had many discussions
11 about scope, and I think that we stayed within the
12 report, within the bounds of the pilot program. I
13 think much of the discussion was focused on the fact
14 that the FIPP's and recommendations like this would
15 be well served to be included within a broader set
16 of cybersecurity programs. We did not include them
17 here because of the scope issue.

18 MS. SOTTO: More comments or questions
19 from the committee?

20 (No response.)

21 MS. SOTTO: Dan, may I ask you to please
22 read slowly for the committee the two amendments

1 that were just discussed? Because I'm going to then
2 ask for a vote of the committee.

3 MR. CHENOK: Yes, if I can find where I
4 wrote them.

5 The first amendment on page 11 in the
6 bullet is in the first bullet, the last unbulleted
7 clause of that bullet, after the terms "assess the
8 program," delete the apostrophe "s" and the words
9 "intended purpose." So it reads: "If a pilot
10 cannot effectively assess the program, then it is
11 not worth any intrusion into privacy rights."

12 The second amendment would be to add a new
13 bullet immediately following that clause which says:
14 "If effectiveness has not been established and the
15 program is deemed not worthwhile, we recommend that
16 DHS not collect PII or the content of private
17 communications as part of the program."

18 MS. SOTTO: Okay. Comments or questions
19 about those two amendments?

20 (No response.)

21 MS. SOTTO: Okay. Hearing none, I would
22 ask for a formal motion, please, to approve the

1 paper as amended as a report that's been adopted by
2 the full committee.

3 MR. PIERSON: I'll put forth a motion that
4 it be adopted.

5 MS. GATES: I'll second.

6 MS. SOTTO: Please say aye if you approve
7 it.

8 (Chorus of ayes.)

9 MS. SOTTO: We have a consensus and a vote
10 to release the paper. Congratulations.

11 MR. CHENOK: Thank you all for your time.

12 MS. FRANKLIN: Thank you very, very much.

13 (Applause.)

14 MS. SOTTO: And please do not disband as a
15 subcommittee. We need you and we would like the
16 opportunity to look to you in the future. Thank you
17 so much.

18 MR. CHENOK: We are here to serve.

19 MS. SOTTO: All right. We're going to
20 turn to the next part of our agenda. The Technology
21 Subcommittee also received a tasking in April 2012.
22 The full committee received the tasking asking us to

1 research what privacy considerations the Department
2 should include in determining if the collection and
3 use of a biometric is warranted, and if so, what
4 privacy protections the Department should consider
5 when using biometrics for identification purposes.
6 We are, of course, aware that US-VISIT is DHS's
7 primary provider of biometric identification and
8 analysis services, and we're familiar with US-
9 VISIT's robust privacy policies and practices.
10 We've heard about those practices a number of times.
11 This tasking, though, allowed us to consider
12 possible ways to improve or expand on these privacy
13 practices as more biometric identifiers are
14 considered by the Department.

15 David Hoffman chairs the Technology
16 Subcommittee, and the subcommittee has now completed
17 its research. And before I turn to David, I would
18 like to thank Joanna Grama for stepping in to lead
19 the subcommittee on an interim basis while David was
20 out on sabbatical. And this committee has really
21 done a stupendous job in a quick period. So, David,
22 thank you for your leadership and please tell us

1 about the paper.

2 MR. HOFFMAN: So I think it's nice to be
3 thanked for the leadership of stepping out when
4 stepping out and taking a sabbatical.

5 (Laughter.)

6 MR. HOFFMAN: I'm more than willing to do
7 that again if needed.

8 And so I'd like to echo the thanks to the
9 subcommittee and particularly to Joanna. It was
10 nice to come back and find the paper in such
11 tremendous shape from the efforts of many members of
12 the subcommittee.

13 As Lisa stated, what we were asked to do
14 was specifically to provide guidance on privacy best
15 practices associated with the use of biometrics, and
16 in line with that, there were two specific questions
17 that we addressed. The first was what privacy
18 considerations should DHS include to determine
19 whether the collection and use of a biometric is
20 warranted? And the second was what specific privacy
21 protections should DHS consider when using
22 biometrics for identification purposes?

1 To do that, while I was out on sabbatical,
2 the subcommittee had several meetings and received
3 briefings on potential uses of biometrics by the
4 Department. And so specifically, there were
5 meetings with the Science and Technology Directorate
6 and also meetings with US-VISIT. But to be clear,
7 this paper was not a review of any specific program
8 or a gap analysis of any particular implementation.
9 Those reviews were done to provide examples of what
10 was being done to determine what best practices
11 should be, and that's what this paper is directed
12 at. So it in no way should be interpreted as any
13 statement that any of the things in this paper are
14 actually things that are currently not going on.

15 So we then approached the paper first with
16 a need to provide a scope of what we meant by
17 biometrics, and you can see that on page 1 of the
18 paper. We say it refers generally to the science of
19 measuring, recording, and analyzing a person's
20 unique physical attributes. And then we give
21 examples of what those unique biometric and physical
22 attributes can be, but those are merely examples.

1 We wanted to define biometrics rather broadly.

2 We then proceeded to address the first
3 question which was what privacy considerations
4 should DHS include in determining the collection and
5 use of a biometric is warranted. And what we
6 recommended there was a four-step analysis and said
7 that we thought that it would be warranted for DHS
8 to follow a selective and cautious approach here.
9 The four steps specifically were to: number one,
10 evaluate the usefulness and utility of a biometric
11 method; second, recognize the potential privacy
12 impacts of biometric use; third, review program
13 requirements of biometric use; and fourth, consider
14 the risks and benefits of deploying biometrics.

15 So the first, evaluating the usefulness
16 and utility of a biometric, similar to the
17 discussion we just had about the Cybersecurity
18 Subcommittee paper. If there is no utility from
19 collecting and using the biometric, obviously, then
20 it does not need to be done. That's the first step
21 in the analysis.

22 The second, recognizing the potential

1 privacy impacts of biometrics. We thought what
2 would be useful here would be to give a series of
3 examples of the factors that could impact privacy,
4 recognizing that this is a non-exclusive list. And
5 you can see the list of those on page 3 of the
6 report.

7 We then proceeded to analyze the steps
8 that should be taken to review the program
9 requirements and steps to be used in considering
10 risks and benefits for deploying biometrics,
11 including a model. It's a recommended model, noting
12 when would be a useful time to go forward with using
13 a biometric, specifically pointing to the fact that
14 there would be low risk and high benefit, and that
15 any other quadrant of this two-by-two analysis would
16 require much closer inspection of whether this
17 should be done, and if it was obviously in a high-
18 risk and low-benefit situation, that we would
19 recommend against proceeding with that type of a
20 program.

21 We then turned ourselves to the second of
22 the tasking questions and looked at our recommended

1 privacy protections for biometric use for
2 identification purposes. Similar to the approach
3 that was taken by the other committees, we used the
4 framework document that was published in 2006 by
5 this committee to analyze the issue. And within
6 that framework document, there is a reference to
7 analyzing these issues through the Fair Information
8 Practice Principles. So we give some background in
9 the document on the Fair Information Practice
10 Principles. And recognizing that different
11 organizations over time since the 1970's have
12 defined the Fair Information Practice Principles
13 differently, we wanted to make clear that we are
14 referring to DHS's specific implementation of the
15 Fair Information Practice Principles, which was
16 completed in a report, I believe, also in 2006,
17 which is footnoted in this document.

18 We then take each one of the Fair
19 Information Practice Principles that's been ratified
20 at DHS and do an analysis of how those apply to
21 biometrics. So that was transparency, individual
22 participation, purpose specification, data

1 minimization, use limitation, data quality and
2 integrity, security and accountability and auditing.
3 As a result of that analysis, we came up with 15
4 recommendations, and I will read and list those
5 recommendations now.

6 First, DHS, when considering use of
7 biometrics, should develop a strategy of policies
8 and procedures to provide adequate notice, including
9 the specific legislative authority for collecting
10 the biometric and the intended purpose for the
11 collection.

12 Number two, provide employees with
13 training to ensure adequate notice.

14 Three, deploy written notices in different
15 languages.

16 Four, use standard images and icons to
17 communicate the use of biometrics.

18 Five, audit operational notice processes
19 regularly to ensure they are consistent with policy.

20 Six, engage in a public education campaign
21 to explain the necessity of DHS use of biometrics.

22 Seven, limit use of the biometric to those

1 specific purposes described in the notice.

2 Eight, minimize collection of biometrics
3 to only data that is necessary for the stated
4 purpose and only retain such data for the period
5 necessary for such purpose.

6 Nine, develop a strategy to periodically
7 assess the accuracy of the collection methods and
8 technology.

9 Ten, technology used to collect and
10 maintain biometric information should contain
11 customer integrity checks to ensure accurate and
12 complete capture of information.

13 Eleven, systems that maintain biometric
14 information should have appropriate technical
15 controls to help ensure accuracy.

16 Twelve, any plan to use biometrics should
17 include at least the following security elements:
18 secure collection devices limiting the transmission
19 and storage of biometric images on collection
20 devices; databases used to store biometric should be
21 secured according to industry best practices for
22 highly sensitive data; and replication of original

1 biometric should be avoided.

2 The thirteenth recommendation. The
3 Privacy Office should be included early on in any
4 consideration of the use of biometrics.

5 Fourteenth, the Privacy Office should
6 analyze the privacy threshold analysis and the
7 privacy impact assessment processes to make certain
8 they sufficiently focus on biometric data.

9 And fifteen is the Privacy Office should
10 ensure periodic compliance reviews are conducted to
11 make certain biometric implementations are
12 appropriately.

13 I'd like to highlight the last three of
14 those recommendations. While all the
15 recommendations are important, I think those are
16 particularly critical recommendations to make sure
17 that privacy protections are going to be integrated
18 sufficiently over time into different programs as
19 they are launched and as they are updated and
20 maintained to further DHS's mission.

21 So that is the summary of the document.

22 Since we have sent the document out for

1 review, I have been provided by different members of
2 the committee with three very specific edits that I
3 do believe need to be made. One is a typo and two
4 are very helpful, additional explanatory pieces to
5 make clear the points that we are making. Let me
6 provide those now slowly for everyone for your
7 consideration.

8 The first is on page 4 of the document
9 between lines 15 and 16, and this is a typo that
10 somehow, when we were updating the document, we
11 deleted one of the subject headings. So this should
12 be subject heading number 3 that occurred on page 2
13 when we laid out the four elements of our approach.

14 And so it should be "review program requirements
15 and biometrics use," and that should be underlined.

16 The next edit is on page 5. It is on line
17 8. Let me go up to line 5 and read. This is how
18 this will flow. It says: "The following risk-
19 benefit model is offered to help DHS analyze these
20 factors. In this model, the risk-benefit balance
21 may point to a clear decision of deploy or don't
22 deploy in some cases. However, other situations

1 demand further review and diligence regarding
2 specific program requirements and objectives, and
3 the potential privacy impact" -- this is the
4 addition. "And the potential privacy impacts of
5 using biometrics to meet those requirements and
6 objectives." Let me read that again because I read
7 that quickly. "And the potential privacy impacts of
8 using biometrics to meet those requirements and
9 objectives." Then there will be a period.

10 The last of the three edits is on the same
11 page. It is in line 32. Here we describe the
12 privacy risk, and then we just refer to harm done.
13 I think it's actually a good change to make clear
14 that the harm done there that we are referring to is
15 "potential privacy impacts/harm." So that would
16 replace the two words "harm done" with "potential
17 privacy impacts/harm." And at the end of that
18 sentence after the semicolon, it would read "and the
19 potential privacy impacts/harm," if others have
20 known or have, slash, know this collected biometric.

21 So that is the summary of our report, and
22 I'm open for any questions or comments.

1 MS. SOTTO: Barry?

2 MR. STEINHARDT: A really excellent
3 report. I thought you did a terrific job.

4 I have one question, though. I'll repeat
5 that. A really excellent report. I want to get
6 that on the record and make sure everyone hears
7 that.

8 I do have one question which is why the
9 report doesn't discuss the issue of one-to-one
10 biometric identification as opposed to one-to-many.
11 By that I mean -- I'll give you an example. It
12 would be possible, for example, at a checkpoint to
13 examine someone's passport, say, a photograph and a
14 passport, compare that to an image that is captured
15 at the location to determine that the person who is
16 presenting the passport is the same person whose
17 photograph is in the passport as opposed to a check
18 of a database where you're checking to determine
19 whether or not that is the person among many people.
20 It could be thousands. It could be tens of
21 thousands of people. I mean, as a general matter a
22 one-to-one, when it's possible to do that, as the

1 advantage, A, of being less privacy intrusive. You
2 don't need to create a database to do it. And two,
3 in many cases it could be more accurate. You would
4 get a better result with a one-to-one check or one-
5 to-few check as opposed to a one-to-many check in
6 face recognition which is at the moment the
7 principal biometric that DHS uses.

8 I am just wondering if you've thought
9 about having a discussion of that, if you're open to
10 including a section or a sentence or two that
11 discussed that that perhaps state whether this is
12 right, whether there's a preference for using the
13 one-to-one where that's feasible.

14 MR. HOFFMAN: Let me make sure I
15 understand the recommendation. Let me make sure I
16 understand the recommendation first, and I'll do
17 that by way of describing a little bit of the scope
18 of what we were trying to accomplish.

19 As I noted in how we drafted the
20 introduction, we wanted this paper to apply to a
21 very broad scope of the potential types of programs
22 that could use biometrics and could need to have

1 privacy protections put in place. Some of those
2 could potentially be one-to-one. Some of those may,
3 by their nature, need to be one-to-many. So this is
4 not what you said. And so I'm admitting I'm not
5 trying to put words in your mouth, but I want to
6 come back and say is where you want to go with that
7 to say, look, it would be good to have a
8 recommendation in here to say when you're looking at
9 a one-to-many proposal for a program, there should
10 be a step in the analysis to say could you
11 accomplish the program with it still being one-to-
12 one because that's more privacy sensitive?

13 MR. STEINHARDT: That is a far more
14 articulate way of saying it.

15 (Laughter.)

16 MR. HOFFMAN: I would love other people on
17 the committee and the subcommittee to speak to that.
18 I will give you my first impressions. I'm not
19 opposed to placing that in here somewhere if we can
20 make clear that it's subject to it still being able
21 to accomplish the mission of the program.

22 MR. STEINHARDT: Absolutely.

1 MR. HOFFMAN: Others' thoughts?

2 MR. PALMER: I absolutely agree.

3 MS. GATES: I recall when we were talking
4 about section 2 and talking about recognizing the
5 potential privacy impacts, we had some discussions
6 on identification systems versus verification
7 systems, which I think, Barry, is what you're
8 driving at.

9 And back to David's comments, we tried to
10 keep our statements here very broad, while we had
11 those conversations and went down roads not unlike
12 where you just went, Barry, we chose to keep the
13 language very broad here. So I think it would be
14 consistent with the discussions we had in the
15 committee if we included something like that though.

16 I think Greg was involved in some of those
17 too so I don't know if you have anything to add.

18 MR. NOJEIM: I don't have anything to add.
19 I do remember the conversations.

20 Let's try to come up with language that
21 operationalizes it.

22 MR. HOFFMAN: I'm not sure this is a

1 perfect fit. I'm trying to think where would be a
2 good place to put this in. I wonder if including it
3 as an example underneath one of the FIPP's as a
4 mechanism for accomplishing --

5 MR. PALMER: Minimization.

6 MR. HOFFMAN: And Charles is listing
7 exactly where I was going which is minimization.

8 Now, minimization here is talking about
9 minimization of collection, and what I think we're
10 getting at with one-to-one is slightly different,
11 which is minimization of matching against what
12 you're matching it against and searching. So I'm
13 not sure that's the right fit, although we could
14 call that out within minimization if we wanted to.

15 MS. GATES: I'm wondering, David, if
16 perhaps back in that recognizing the potential
17 privacy impact section where we have the bullet
18 points and a set of considerations, this might be a
19 scenario to add there and might fit in that
20 conversation rather than trying to fit it into a
21 single one of the FIPP's.

22 MR. PALMER: Especially since it's a point

1 of, as Barry said, one-to-one. It's an imperfect
2 science. One-to-one is pretty good. One-to-many --
3 it's I am who I say I am. That is one-to-one. That
4 is not so bad. You guess who I am. That's the
5 tough one and that's a lot harder and much more
6 subject to error in the scenarios that are in here
7 with the numbers. So I think you're right. It
8 would make sense to make it a little scenario if we
9 could just think of a way to say what he did, what
10 David did, which is if it's possible to do one-to-
11 one, try.

12 MR. HOFFMAN: So I'd like everybody to
13 take a look at page 5 because I really like this,
14 and if we look at line 12 and think about whether we
15 could add something to the end of this paragraph,
16 since that is a place where it's specifically saying
17 the analysis should also look for reasonable
18 mechanisms to mitigate risk prior to making any
19 implementation decision and then to add something.
20 And I'm drafting on the fly here. For example, if a
21 program wishing to use a biometric can be
22 accomplished with a one-to-one matching instead of

1 one-to-many matching, then the program should take
2 the least privacy impactful approach.

3 MR. STEINHARDT: Should use one-to-one.

4 MR. HOFFMAN: Should use one-to-one. Does
5 anybody object to including it there? Then we can
6 try to wordsmith it.

7 MS. SOTTO: The only thing I might add is
8 that we need to define one-to-one.

9 MR. PALMER: We can easily -- it's subtle.
10 On the bottom of page 2, you talk about varying
11 rates of success and authentication and
12 identification. Authentication is one-to-one.
13 Identification is one-to-many. I could spell it
14 out.

15 MR. HOFFMAN: Say that again, Charles?

16 MR. PALMER: Authentication is one-to-one.
17 I really am Charles. And identification is you
18 guess who I am.

19 MR. HOFFMAN: So if we were to say could
20 be accomplished with an authentication --

21 MR. PALMER: Well, that's a term of art.

22 MR. HOFFMAN: -- instead of an

1 identification mechanism.

2 MR. PALMER: We should spell it out. It's
3 a term of art. We should spell it out. But that's
4 really what I was saying here.

5 MR. NOJEIM: For people on the phone, I
6 just want you to know Shannon is doing a great job
7 so you can hear what we're saying. Maybe you should
8 put the phone on wheels.

9 MS. WEINBERGER: Or Shannon.

10 (Laughter.)

11 MS. WEINBERGER: Do we want to speak to
12 the diminished validation return you get from the
13 one-to-many? Because I think that's what you're
14 getting at. One-to-one is the person in front of
15 you. It's very easy to determine. You don't have
16 to troll through millions in a database like a
17 facial recognition database. A facial recognition
18 database has -- mine has more than 20 million faces
19 within it, and it runs a daily report telling me
20 when anyone comes in to get a driver's license that
21 these are the 50 people who meet the 19 points of
22 verification on that, and you'd be surprised how

1 different these people look and it takes human eyes
2 on a daily basis to go through all 50 to 150
3 printouts to say the person who took a picture is
4 not this person over here. They are completely
5 different, but they met the 19-point requirement.
6 So I think you want to talk about the diminished
7 value when you have one-to-many.

8 MR. PALMER: I don't disagree. It could
9 very well be that it depends on your perspective.
10 If you're the agent in the situation trying to
11 figure out if that really is Barry, if you can use
12 this to produce the space that you have to look at
13 from 19 million to 9, then that's a win.

14 MR. HOFFMAN: I'm inclined to also believe
15 that that really depends upon the purpose of the
16 program and what they're trying to accomplish. I
17 think in many instances that would be case. In
18 some, though, specifically identification against a
19 large group of actors could be what they're trying
20 to accomplish.

21 I just tried to draft something. Let me
22 read it slowly. I have at this point specifically

1 no pride in authorship. At the end of line 12,
2 adding onto the existing paragraph on page 5, say,
3 "for example, if a program wishing to use a
4 biometric can be accomplished with one-to-one
5 matching (e.g., a matching of a photo to another
6 specific photo in a database for authentication
7 purpose), instead of one-to-many (e.g., a matching
8 of a photo to a database of photos to identify an
9 individual) then DHS should pursue the one-to-one
10 approach."

11 MS. GATES: I'm just wondering if instead
12 of "program" -- we talked about program objectives
13 and requirements throughout the paper. So perhaps
14 something like, "for example, if program
15 requirements and objectives can be met."

16 MR. HOFFMAN: So the beginning of that
17 sentence would read: "For example, if a program's
18 objectives can be accomplished with one-to-
19 matching." And then proceed on.

20 MS. GATES: Perhaps "requirements and
21 objectives."

22 MR. HOFFMAN: What does requirements give

1 you there that objectives doesn't?

2 MS. GATES: I'm wondering if we may be
3 duplicating there. We've just been talking about
4 requirements and this is there in that section. But
5 I look to others for do you think we really need
6 both terms.

7 MR. HOFFMAN: Or we could use
8 "requirements" instead of "objectives."

9 MS. GRAMA: I like "objectives," but we
10 have, throughout the paper, used the term "program
11 requirements" particularly in the four steps.

12 MR. HOFFMAN: It seems to me that they're
13 synonymous and we could put "requirements" in
14 instead of "objectives."

15 Does anyone have a strong opinion? I'm
16 going to put "requirements."

17 Any other comments on that addition?

18 MR. STEINHARDT: When you talked about
19 that addition, you're talking about that specific
20 program versus requirements.

21 MR. HOFFMAN: Or anything on this
22 particular --

1 MR. STEINHARDT: I would take out the
2 first reference there to database. As I recall the
3 language used, it was something like, for example, a
4 matching or comparing a photograph in a database to
5 a photograph --

6 MR. HOFFMAN: So that first parenthetical
7 could read a matching of a photo to another specific
8 photo for authentication purposes. It doesn't have
9 to be in a database. That's a really good point.

10 MS. PULITO-MICHALEK: Excellent paper. I
11 really enjoyed reading it. I learned a lot.

12 I have two questions for you. One thing I
13 really loved was on page 4 regarding use of
14 biometrics, if it's going to be viewed as
15 unnecessary or intrusive, alternate means should be
16 considered.

17 My first question -- it may be covered in
18 here or this may be the next step. This question
19 may have already been answered. I see the questions
20 on page 2. I see you talking about the usefulness
21 of biometrics and the analysis, but I don't know if
22 that lead question should be is it necessary to use

1 biometrics for the project and why. And it may be
2 covered in here. So I'm not sure. Should that be
3 the initial question, or is this really the phase 2?
4 That question has already been asked and answered
5 and this is the implementation.

6 MR. HOFFMAN: I'll tell you the way I've
7 been reading this, which is to evaluate the
8 usefulness and utility goes to is it necessary, not
9 only is it necessary but is the implementation
10 coherent to accomplish what needs to be done. Maybe
11 that's not the way other people read it. So I'm
12 open to edits.

13 MS. PULITO-MICHALEK: I don't know. It's
14 just one of the things. I was on page 2, and I
15 don't know if you'd get to it later on. I know we
16 talk about it another section, but is it necessary
17 for the project. I think this might be in phase 2.
18 That's already been probably answered. If that
19 wasn't a red flag for anybody else, I'll let it go.

20 I'll jump to my second question. On page
21 7, you talk transparency and disclosure. I was
22 wondering if it came up, the potential to revoke

1 consent. Is it possible for an individual to revoke
2 consent and how we got these processes handled?

3 MR. HOFFMAN: So I think that's a really
4 interesting point. You can think of certain
5 programs, let's say, applying for a permit to
6 transport hazardous substances, where you might need
7 to provide your biometric data to act as an
8 identifier at that point in time, but at the point
9 in time when you no longer want to transport that or
10 need to have that license, it may not be necessary
11 anymore for DHS to have the data. And therefore,
12 you should have the ability to revoke that consent.

13 MR. NOJEIM: As another example, say you
14 want to be a member of DPIAC and they want to
15 collect your fingerprints for that purpose, and then
16 you're no longer a member of DPIAC and maybe you
17 don't want your fingerprints to be in some
18 promiscuously accessed database after you are no
19 longer a member of DPIAC. Should you be able to
20 force the removal of your fingerprints because they
21 can no longer be used for the purpose they were
22 collected? That's a good question.

1 MS. SOTTO: Does anybody disagree or does
2 everybody agree -- let me put it in the positive --
3 that there should be an ability to, where
4 appropriate, revoke consent?

5 MS. GATES: I wonder if this is partly a
6 notice issue because I'm thinking there could be
7 programs and circumstances where it's perhaps
8 impractical or challenging to go and scrub that data
9 out.

10 MS. SOTTO: That's why I'm saying "where
11 appropriate."

12 MS. GATES: So I'm wondering if this is
13 partly a notice issue as well as an individual
14 participation issue.

15 MS. SOTTO: I think this is a very good
16 point. I wonder if we can fix this easily by adding
17 "where appropriate, there should be consideration
18 given to the ability of people to revoke consent.

19 MR. NOJEIM: Then it would be appropriate
20 to allow DPIAC members to revoke consent, where
21 appropriate.

22 (Laughter.)

1 MS. SOTTO: I'll read you again -- well, I
2 don't know where I'm putting it. Say "where
3 appropriate, consideration should be given to the
4 ability of an individual to revoke consent."

5 MR. HOFFMAN: This might lead in very well
6 at the end of line 36 on page 7 because we've got a
7 sentence that talks about refusal to participate,
8 and we might even want to add that. Refusal to
9 participate or withdrawal of consent, that the
10 impact of that should be clearly communicated. Do
11 you want to repeat then what would go in there?

12 MS. SOTTO: Where's the sentence that
13 precedes it? Okay. "In addition, where
14 appropriate, consideration should be given to the
15 ability of an individual to subsequently withdraw
16 consent for DHS to use a biometric."

17 MS. GATES: To retain and continue to use.

18 MR. HOFFMAN: To collect, use, or retain.

19 MS. SOTTO: Collection has already
20 happened.

21 MR. HOFFMAN: There could be subsequent
22 collection. If you said that every time you enter

1 some facility that it's okay to collect, there could
2 be a future collection still I think.

3 MS. SOTTO: To subsequently collect.

4 MR. HOFFMAN: So what I wrote was at the
5 end of line 36, "In addition, where appropriate,
6 consideration should be given to an individual" --

7 MS. SOTTO: "To the ability of an
8 individual" or "the right of an individual."

9 MS. GATES: "To the ability for an
10 individual."

11 MR. HOFFMAN: I don't mind talking about
12 rights. I don't like saying on the record that
13 we're giving people rights necessarily from this
14 committee.

15 MS. SOTTO: "To allow an individual to
16 withdraw."

17 MR. HOFFMAN: "To allow an individual to
18 withdraw consent for DHS to subsequently collect,
19 use, or maintain the biometric." And then in line
20 38 where it says "privileges," "the consequences for
21 the individual's refusal to participate or withdraw
22 consent, should be clearly communicated, as well as

1 the argument for why such participation is
2 mandatory" --

3 MS. SOTTO: Read that one more time.

4 MR. HOFFMAN: Let me read the whole
5 paragraph starting at the beginning of line 34.

6 "Where possible, individuals should have the option
7 not to participate in a program involving the use of
8 biometrics for identification purposes while
9 maintaining the rights and privileges of other
10 individuals who are participating in a program
11 involving biometrics. In addition, where
12 appropriate, consideration should be given to allow
13 an individual to withdraw consent for DHS to
14 subsequently collect, use, or retain the biometric."
15 Then continuing on with the existing line 37, "When
16 participation in the biometrics program is mandatory
17 to receive certain rights and privileges, the
18 consequences for the individual's refusal to
19 participate," adding in "or withdrawal of consent,"
20 comma, should be clearly communicated, as well as
21 the argument for why such participation is
22 mandatory, such as for national security purposes."

1 That's a good catch.

2 MS. SOTTO: Comments on that change?

3 (No response.)

4 MS. SOTTO: It is done.

5 Additional comments or questions? Yes,
6 Barry?

7 MR. STEINHARDT: I'm just wondering if you
8 think it might be useful to have -- and I don't know
9 where it might be placed, but whether it would be
10 useful to have a recognition that in addition to the
11 problem that you discuss quite well and effectively
12 of the false positives, that there's also from a
13 security perspective a down side to using a
14 biometric that has an unacceptably high false
15 negative rate, in other words, lets the bad guys get
16 in. It's entirely possible someone might suggest --
17 why don't we use facial bumps as a way -- phrenology
18 as a way of doing this. Well, part of the reason,
19 of course, we're not doing that is you're not going
20 to find the bad guys that way.

21 MR. HOFFMAN: Would this be something that
22 we could mention in the context of evaluating the

1 usefulness and the utility of using it, just a
2 mention of considering the impact of false
3 negatives?

4 MR. PALMER: It's also laid out in the
5 example at the top of page 3. It's not a specific
6 recommendation. It's just part of a scenario.

7 MR. STEINHARDT: That's what I wanted to
8 be clear about. It referred to the false reject
9 rate. I thought the individual was being rejected
10 because there was a false positive there, not
11 because of false negatives.

12 MR. PALMER: Well, it didn't find their
13 fingerprints. I mean, it should have. They were
14 falsely rejected -- to the fingerprints in the
15 databases. They offered it and they were rejected
16 falsely. It's a false negative. It's a bit of geek
17 speak, I admit.

18 MR. STEINHARDT: I didn't read it that
19 way. It may have been my mistake. But I'm
20 wondering if we couldn't make that clearer by saying
21 something along the lines of "if a biometric system"
22 -- I would actually use the phrase "false negative"

1 because that's sort of a term of art. But if the
2 biometric system has a false reject or a negative
3 rate and then just say, i.e., fails to identify
4 individuals who meet the criteria or who should have
5 been identified, something to clarify what we meant
6 by that.

7 MR. NOJEIM: This is kind of a false
8 positive rate. Right?

9 MR. HOFFMAN: What if on page 2 in line 33
10 -- the sentence starting on line 32 says, "The
11 utility of a biometric depends not only on how well
12 it can reliably and uniquely identify an
13 individual." What if right before the comma we open
14 a parenthetical that said "minimizing false
15 positives and false negatives"?

16 MR. STEINHARDT: I'm not sure I would say
17 minimize. You might say something like identify an
18 individual at unacceptable rates, unacceptable false
19 positive and false negative rates, unacceptably
20 high.

21 MS. SOTTO: We could put, parens,
22 "considering unacceptably high false positives and

1 false negatives."

2 MR. HOFFMAN: Does that sound right,
3 Barry? The sentence is talking about the analysis
4 of it, and so using "considering" instead of
5 "minimizing." Does that work?

6 MR. STEINHARDT: In addition to
7 "considering," I think it should refer to
8 unacceptably high rates.

9 MR. HOFFMAN: So it could be considering
10 whether there are unacceptable rates of false
11 positives and false negatives. False positives or
12 false negatives?

13 MR. STEINHARDT: Or, yes.

14 MS. SOTTO: "Unacceptably high rates of
15 false positives or false negatives."

16 MR. PALMER: And we'll have to say
17 somewhere what that means.

18 MR. HOFFMAN: Do we need to define false
19 positives and false negatives?

20 MR. PALMER: We may have to define it
21 because false positive people can understand, but
22 false negative -- do you think they'll get that? It

1 works for me.

2 MS. SOTTO: Do you want to read that one
3 more time?

4 MR. HOFFMAN: Starting in line 32, "The
5 utility of a biometric depends not only on how well
6 it can reliably and uniquely identify an individual
7 (considering whether there are unacceptably high
8 rates of false positives or false negatives)," then
9 the comma and then continuing on line 33, "but also
10 on how difficult it is to capture."

11 MS. SOTTO: Going once. Okay.

12 Any other comments before we move to a
13 vote?

14 (No response.)

15 MS. SOTTO: Seeing no hands and no tents
16 raised, I would ask for a formal motion, please, to
17 approve this paper as a formal report adopted by the
18 full committee.

19 MS. GRAMA: I make that motion.

20 MS. SOTTO: So moved. Any seconds?

21 MR. PALMER: I second.

22 MS. SOTTO: All in favor, say aye?

1 (Chorus of ayes.)

2 MS. SOTTO: We have a consensus vote.

3 Thank you very, very much to the committee
4 and to David's leadership and Joanna's leadership.
5 Well done.

6 (Applause.)

7 MS. SOTTO: With that, we are turning now
8 to the public comment period of our meeting. If the
9 public would like to address the committee, we are
10 hitting that now. So please come forward if you
11 would like to speak. We do have one commenter from
12 the public. I would ask you to come forward, and
13 that is Jeremy Scott. And why don't you have a seat
14 at the table? And I would ask you to, please, keep
15 your remarks to 3 minutes, as described in the
16 Federal Register notice. Please go ahead.

17 MR. SCOTT: Thank you. My name is Jeremy
18 Scott. I'm the national security fellow at the
19 Electronic Privacy Information Center. I'd like to
20 thank the committee for holding this public meeting,
21 creating the draft reports, and also granting me
22 some time to speak.

1 First, I'd like to recognize the many good
2 recommendations in both the cybersecurity pilot
3 draft report and the biometric use report. I'd like
4 to make just a few quick points that apply to the
5 reports and generally to the committee
6 recommendations.

7 Both the reports mention the Privacy Act I
8 believe, but neither mention the Freedom of
9 Information Act, or FOIA. With respect to the
10 Privacy Act, EPIC would like to encourage the
11 committee to not just encourage compliance but
12 strongly encourage DHS to not exempt records
13 collected under the DHS programs from Privacy Act
14 provisions. And additionally, with respect to FOIA,
15 EPIC encourages the committee to emphasize the need
16 for DHS to adhere to the openness requirements of
17 FOIA. EPIC would like to underscore FOIA's purpose
18 to facilitate transparency by providing public
19 oversight of Government operations.

20 And speaking of transparency, I believe
21 both reports generally recommend transparency and
22 accountability, and these are very good things. But

1 EPIC would like to emphasize how important
2 transparency and accountability is.

3 Now, the Senate report on the fusion
4 centers was mentioned a few times during the course
5 of this day, and that report, I think, highlights
6 the need for very good transparency and
7 accountability. Some of the issues that were
8 highlighted in that report are things that should
9 have come out beforehand. Privacy compliance
10 reviews, privacy impact assessments, and the like
11 are nice, but if they don't actually expose actual
12 issues to the public, then they're not serving their
13 purpose.

14 Additionally, it's nice that the DHS
15 Fusion Center review process caught most of the
16 reports that violated privacy, but there was no
17 accountability from these reports or for these
18 reports. And according to the Senate report, the
19 same people kept submitting Fusion Center reports
20 that actually violated the Privacy Act. Yet, they
21 weren't held accountable at all for these
22 violations.

1 I'll close by pointing out that DHS has
2 the largest mandate to do domestic surveillance and
3 has become of sorts a Big Brother's laboratory with
4 programs like the body scanner program, fusion
5 centers, future attributes screening technology
6 program, the cybersecurity pilot program, biometric
7 collection, et cetera. Now, we might not be
8 actually at the point of Big Brother, but
9 nonetheless, it's very important to combat any
10 abuses and unnecessary expansion of DHS, and
11 adherence to the Privacy Act and FOIA, along with
12 strong transparency and accountability programs are
13 absolutely necessary. They not only protect privacy
14 and civil liberties, but they also weed out
15 unnecessary or ineffective programs.

16 Thank you for your time.

17 MS. SOTTO: Thank you very much, Mr.
18 Scott. We will take your comments under advisement.

19 And I would ask members of the public to
20 remember that you may submit written comments at any
21 time. The e-mail address for doing so is
22 privacycommittee@hq.dhs.gov.

1 With that, I would like to express my deep
2 thanks to the speakers and members of the committee
3 who worked so hard over the last few months to
4 complete these papers and work on committees that
5 are in the process of completing papers.

6 This concludes the public portion of the
7 meeting. And we're very grateful for the public's
8 interest in our work, and we hope you will continue
9 to be interested. Minutes of the meeting are going
10 to be posted on the Privacy Office's website at
11 dhs.gov/privacy in the near future, and we would
12 absolutely encourage you to follow the committee's
13 work, check back on the website frequently.

14 And with that, I would ask members of the
15 public to please leave the room so that we can have
16 an administrative session of the committee. And
17 once again, I extend the committee's thanks to our
18 speakers and to those of us who worked so hard on
19 the papers, particularly our Cybersecurity
20 Subcommittee. Thank you so much.

21 (Whereupon, at 4:20 p.m., the meeting was
22 adjourned.)

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21