U.S. Department of Homeland Security
Privacy Office

Data Privacy and Integrity Advisory Committee (DPIAC)
Public Meeting

February 21, 2017
Via Teleconference

Transcribed by:
Alderson Court Reporting
Washington, D.C. 20036
(202) 289-2260

Table of Contents

Committee Members Present on the Call:

Lisa J. Sotto, Chair
Jim Adler
Sharon A. Anolik
K. Suzanne Barber
Craig W. Bennett
Allen Brandt
Alan Broder
James M. Byrne
Joshua Galper
Melodi (Mel) M. Gates
Lynn Goldstein
Joanna L. Grama
Debbie Matties
Joanne McNabb
Sarah Morrow
Charles Palmer
Julie Park
Christopher Pierson
Tracy Ann Pulito-Michalek
Russell Schrader
Jeewon Kim Serrato
C.M. Tokë Vandervoort
Marjorie S. Weinberger
Richard Wichmann

Other Participants:
Jonathan Cantor

PROCEEDINGS

Agenda Item: Roll Call

MS. SANDRA TAYLOR: Okay. Good morning. It is now 10:03 a.m. on Tuesday, February 21st.

This is Sandy Taylor. I am the Designated Federal Official for the Data Privacy and Integrity Advisory Committee. This is our public meeting.

I'm going to begin the meeting by taking a roll of our committee members. When I call your name, just say "here." Please speak loud because we do have a court reporter online who's taking minutes for this meeting.

It's --

[Audio feedback.]

MS. SANDRA TAYLOR: I'm sorry? Okay. I'm going to begin by taking roll.

Lisa Sotto?

[No response.]

MS. SANDRA TAYLOR: Hi. Did Lisa just join the meeting?

MR. RUSSELL SCHRADER: Hi. It's Russell Schrader. How are you?

MS. SANDRA TAYLOR: Hey, Russ. Give me one second. I'm going to take a roll of all of our members, okay?

MR. RUSSELL SCHRADER: Okay.

MS. SANDRA TAYLOR: I want to make sure Lisa is on the line. As our chairperson, she should be on the line. Again, if you're typing, please mute your phone.

Has Lisa joined the call?

[No response.]

MS. SANDRA TAYLOR: Okay, guys. I'm going to give it a couple more minutes so Lisa can join the call. Again, please place your phone on mute. I'm going to try to give her office a call to see where she is.

[Pause.]

MS. LISA J. SOTTO: Hello?

MS. SANDRA TAYLOR: Hello.

MS. LISA J. SOTTO: Oh, hi. It's Lisa.

MS. SANDRA TAYLOR: Oh, good. Okay, Lisa. Good. Good.

MS. LISA J. SOTTO: Yeah.

MS. SANDRA TAYLOR: This is Sandy. Okay. I am -- again, this is a public meeting of the Data Privacy and Integrity Advisory Committee. Today is Tuesday, February 21st.

I'm going to start the meeting by taking a roll of our members. When I call your name, just say "here" or "on the line" or whatever. I hope everyone had a good weekend, too.

Lisa Sotto?

MS. LISA J. SOTTO: I'm here. Thank you.

MS. SANDRA TAYLOR: Jim Adler?

[No response.]

MS. SANDRA TAYLOR: Sharon Anolik?

MS. SHARON A. ANOLIK: I'm here.

MS. SANDRA TAYLOR: K. Suzanne Barber?

MS. K. SUZANNE BARBER: I'm here.

MS. SANDRA TAYLOR: Craig Bennett?

MR. CRAIG W. BENNETT: Here.

MS. SANDRA TAYLOR: Allen Brandt?

MR. ALLEN BRANDT: Good morning. Here.

MS. SANDRA TAYLOR: Good morning. Alan Broder?

MR. ALAN BRODER: I'm here.

MS. SANDRA TAYLOR: James Byrne?

MR. JAMES M. BYRNE: I'm here. Thank you.

MS. SANDRA TAYLOR: Joshua Galper?

MR. JOSHUA GALPER: I'm here. Thanks.

MS. SANDRA TAYLOR: Melodi Gates?

MS. MELODI M. GATES: I'm here. Thanks.

MS. SANDRA TAYLOR: Lynn Goldstein?

MS. LYNN GOLDSTEIN: Here.

MS. SANDRA TAYLOR: Joanna Grama?

MS. JOANNA L. GRAMA: Good morning. I'm here.

MS. SANDRA TAYLOR: Debbie Matties?

MS. DEBBIE MATTIES: I'm here.

MS. SANDRA TAYLOR: Joanne McNabb?

MS. JOANNE MCNABB: Here.

MS. SANDRA TAYLOR: Sarah Morrow?

MS. SARAH MORROW: I'm here. Good morning.

MS. SANDRA TAYLOR: Good morning. Charles Palmer?

DR. CHARLES PALMER: Yes, good morning all.

MS. SANDRA TAYLOR: Good morning. Julie Park? Julie Park?

[No response.]

MS. SANDRA TAYLOR: Christopher Pierson?

DR. CHRISTOPHER PIERSON: Hi, everyone.

MS. SANDRA TAYLOR: Hi. Tracy Ann Pulito?

MS. TRACY ANN PULITO-MICHALEK: I'm here.

MS. SANDRA TAYLOR: Russell Schrader?

MR. RUSSELL SCHRADER: Here.

MS. SANDRA TAYLOR: Jeewon Kim Serrato? Jeewon?

[No response.]

MS. SANDRA TAYLOR: Tokë Vandervoort?

MR. JAMES M. BYRNE: This is Jim Byrne. I just got an email from her. She's trying to log on right now. Thanks.

MS. SANDRA TAYLOR: Is that Tokë?

MR. JAMES M. BYRNE: No, this is Jim Byrne. I wanted to let you know. She's trying to log on, and she should be on in a minute or so. Sorry.

MS. SANDRA TAYLOR: Okay. Thank you. Thank you.

Marjorie Weinberger?

MS. MARJORIE S. WEINBERGER: Good morning from Boston.

MS. SANDRA TAYLOR: Good morning. Richard Wichmann?

MR. RICHARD WICHMANN: Here.

MS. SANDRA TAYLOR: Great. Okay. With that, we have enough members so we can go forward with our meeting.

I'm just going to remind everyone to please mute your phones. If you have a question, just indicate it on the screen, and we will definitely try -- we will get to it.

Please remember to keep the acronyms to a minimum. We have people who are first-time attendees or who are not familiar with Government lingo. So please remember to keep the acronyms to a minimum.

Also please remember to keep your phones on mute unless you're actually speaking.

With that, I'm going to turn this -- I'm going to turn the meeting -- oh, before I turn

it over to Lisa, who is our chairwoman, I'm going to turn it over to Jonathan Cantor, who is our Acting Chief Privacy Officer. Jon?

Agenda Item: Opening Remarks

MR. JONATHAN CANTOR: Good morning, everybody. Can you hear me?

FEMALE SPEAKER: Yes.

MR. JONATHAN CANTOR: Okay. Good.

MS. SANDRA TAYLOR: Yes.

MR. JONATHAN CANTOR: Okay. Good morning, everybody. Thanks for getting together today.

Back in September of 2015, former Chief Privacy Officer Karen Neuman asked the Data Privacy and Integrity Advisory Committee (DPIAC) to get together and put together some written guidance on best practices for notifying individuals impacted by a large-scale data breach. I think a lot of us remember what was going on in that period of time, that DHS and the Government writ large through the Office of Personnel Management (OPM) were experiencing a lot of activities as a result of some very, very big data breaches.

And I think, if folks remember, that the Federal Government at that period of time did not have a very modern data breach framework. Ours had been developed in 2007 based on some old 2007 Office of Management and Budget (OMB) guidance. DHS had had some attempts at keeping it current, and we knew that OMB was working on updating its guidance based on what had happened. But we thought it was a good time, given that that was happening, to get some input from experts outside of Government to help us while we were in the process of getting ready to refresh, given that we knew OMB was going to come out with a new policy framework.

So the draft recommendations here, which I am hoping you all will talk about and elaborate on and adopt today, those will -- are very timely. OMB, right at the end of the last administration, did finalize that memo, will kind of come together right with that as DHS begins to, you know, deliberate and circulate a new breach notification process. So they're very timely as we're getting into that process.

So we're really looking forward to these. The timing worked out perfectly. So I was excited to read them, and I'm looking forward to hearing more about it, listening to you deliberate on them so that we could get to work on our important work so that, unfortunately, the next time that I'm afraid this will happen, we'll be ready for it, and we can respond quickly and appropriately.

So, with that, I'm going to turn it back over to Lisa and let you guys get started on this important deliberation.

MS. LISA J. SOTTO: Thank you so much, Jonathan.

And I'll take it just for a brief moment because the real leader of this effort was Joanne McNabb with the Policy Subcommittee, who took this tasking very seriously and over the course of a few months devised, crafted this paper that really has the benefit of years of thinking about data breaches. As everybody knows, we have a very mature data breach notification regime in the United States, much, much less mature overseas. But because we've been dealing with data breaches now for I would say 17-plus years at a national level and a couple more in California -- and Joanne, of course, is the perfect person to lead this charge because she is a leader in the privacy community in California -- we have real wisdom, I think, to impart on data breach notification rules of the road.

So, with that, I will turn it over to Joanne to describe the paper, and we're happy to take any questions.

Thank you.

Agenda Item: Deliberations on Best Practices for Data Breach Notification Report

MS. JOANNE MCNABB: Great. So I'll just sort of highlight some of the points in this.

Thank you, Lisa, and thank you, Jon and Sandy.

As Jon explained, we were given this task many months ago, and we were specifically asked to respond to four questions to -- and those questions were -- are enumerated in the paper. The first being what criteria should the DHS Privacy Office consider when making a decision on whether and when to notify in the case of a potential data breach?

And the second is once that decision has been made, then what are the best practices about source of the notice, the content of the notice, and the delivery mechanism for the notice?

And the third question is about the possibility of "over notifying." The fourth is asking for recommendations on what other supplemental practices should be followed in addition to notification of a breach?

So I think Jonathan gave a good background on the data breach response, particularly regarding the Federal Government. And we noted that there are

many excellent documents available, both from the Federal Government, from State governments, and from the private sector on procedures for responding to a data breach, and we outlined in the paper what the basic data breach response plan consists of. I don't think I need to go over that because I'm sure everyone on the committee is very familiar with that, unfortunately.

And then we decided, given the availability of this kind of general information, that we would limit our recommendations here to the four specific questions that we were asked and rather than cover the full scope of policies and procedures involved in responding to a data breach. So going through the questions, now I'm on the second page of this paper.

The first one on making the decision. Oh, we also note here that after we had completed a draft, then the new Office of Management and Budget memo came out on preparing for and responding to a breach of personally identifiable information. So we went through our draft, made a couple of little changes, but it didn't -- it didn't actually require substantive changes, significant changes in our original draft. So we regard these recommendations as supplementing that memo.

So on the first question of how do you decide whether or not to notify, we spoke to the need to conduct a risk assessment, specifically assessing the risk of harm to the individuals potentially affected rather than, for example, the risk of embarrassment to the organization.

And we also made a recommendation that DHS consider adopting a policy that's present in most of the State breach laws of allowing for a good faith employee exemption. That is in a case where an employee or an agent acting on behalf of the Department inadvertently receives information that they aren't authorized to receive, provided that that employee or agent does not use it in any way or further disclose it, that would be considered not to be posing a risk of harm to the data subjects, and therefore, notification in that case would not be required. So we recommend that you consider adopting that kind of a policy.

I also want to -- I guess this is the way to do it -- make two little edits to that paragraph, the second paragraph under the section of -- Section 1, making the notification. Making the decision to notify. The second paragraph that starts, "In addressing the level of risk." In the third line where it says not -- "such a provision allows for not notifying affected parties." I think that should really be "data subjects" because the assumption in this good faith employee exemption is that the data subjects are not affected.

And then in the last line of that paragraph also just delete "affected" before "data subjects" at the end of that sentence.

MS. SANDRA TAYLOR: Hey, Joanne, this is Sandy. If you could give me one

second?

MS. JOANNE MCNABB: Yeah.

MS. SANDRA TAYLOR: Hey, Heela, did you get Joanne's recommendations to make that change?

HEELA HAMIDI: I think I got it, and it was starting at the risk analysis paragraph.

MS. JOANNE MCNABB: The second paragraph that starts -- the second paragraph under -- on page 2 under point 1. So it's the paragraph that starts, "In assessing the level of risk."

HEELA HAMIDI: Okay.

MS. JOANNE MCNABB: So keep going, it's the third line of that paragraph where it says "not notifying affected parties."

HEELA HAMIDI: Uh-huh.

MS. JOANNE MCNABB: Change "affected parties" to "data subjects."

HEELA HAMIDI: Data subjects. Okay.

MS. JOANNE MCNABB: And then in the last line of that paragraph, the third word from the end, "affected," cross that out.

HEELA HAMIDI: And then cross out "affected." Okay.

MS. JOANNE MCNABB: Yeah. Okay.

MS. SANDRA TAYLOR: Okay. Thanks, Joanne. I want to -- give me one second, Joanne.

I just want to remind everyone before you begin to speak to please announce yourself. Announce your name. Again, this meeting is being recorded, and we just want to make sure that the reporter is getting everything accurately, okay?

Thank you. Go ahead, Joanne. I'm sorry.

MS. K. SUZANNE BARBER: This is Suzanne --

MS. JOANNE MCNABB: So I was thinking there should be -- the committee members should be able to speak at any point, right? So if anybody has any comments on this up to this point, please make them.

MS. SANDRA TAYLOR: Yes. Make them, but just make sure you announce your name.

MS. K. SUZANNE BARBER: This is Suzanne Barber. Just a quick question.

In making this recommendation, was there any discussion about the insider threat issue of -- and assessing that threat as it's becoming an increasing problem within breach issues?

MS. JOANNE MCNABB: Regarding the good faith employee exemption or --

MS. K. SUZANNE BARBER: Yes.

MS. JOANNE MCNABB: Yeah. I don't believe we discussed that. But the idea is that in adopting such a policy, you would be -- part of it would be that the employee didn't use the information or further disclose it. So if there's any evidence the employee was using, i.e., abusing the information, then that wouldn't count. That wouldn't be subject to the exemption.

MS. K. SUZANNE BARBER: Okay.

MS. JOANNE MCNABB: Do you think there's a stronger way to say that?

MS. K. SUZANNE BARBER: Maybe to say exactly that. I just see an increasing concern and an issue with we've been doing some research at 30 percent of the breaches involve an insider threat. So --

MS. JOANNE MCNABB: Hmm, that's sort of surprising. Do you include by "insider threat" victims of phishing? Employee victims of phishing?

MS. K. SUZANNE BARBER: It is -- no.

MS. JOANNE MCNABB: You mean actual intentional employee abusers?

MS. K. SUZANNE BARBER: Yes.

MS. JOANNE MCNABB: Yeah.

MS. K. SUZANNE BARBER: So, anyway, it's --

MS. SANDRA TAYLOR: Okay. Who's speaking?

MS. K. SUZANNE BARBER: This is Suzanne Barber with the University of Texas. But anyway, I don't want to hold up the conversation, but maybe just some acknowledgment. And what you said was, it seemed to me, very appropriate that if there wasn't evidence of abuse after the risk assessment that,

indeed, it was accidental. And that happens a lot, too. And I understand the recommendation.

MS. JOANNE MCNABB: Mm-hmm.

MR. RICHARD WICHMANN: This is Rick Wichmann. Joanne, sort of on that same note, in the next paragraph, top of page 3, typically, I'm coming from a Health Insurance Portability and Accountability Act (HIPAA) perspective or for a health insurance company. And it shows the nature of the data subject but does not -- does not cover the nature of the unauthorized access.

So maybe it's in there that you can -- you know, was this a contractor --

MS. JOANNE MCNABB: Yeah, I -- yeah, yeah. Yeah, that's a good point, I think. Does anybody else on the subcommittee have thoughts about that?

MS. SARAH MORROW: Yes, this is Sarah Morrow. In that first sentence where you say risk analysis would include assessing the nature of the data, couldn't we also add the nature of the threat, and wouldn't that take care of it?

MS. JOANNE MCNABB: Yeah. Yeah. The -- so maybe put it at the end or -- wait. So how about putting it, adding it onto the end of the second sentence that starts, "Other factors consider the nature of the data subjects," da-da-da, comma, "and the nature of -- of the attackers?" Or "the threat" seems a little broader than what we're trying to get out there. Of the -- of the what?

MS. K. SUZANNE BARBER: I like threat. Oh, this is Suzanne Barber.

MS. JOANNE MCNABB: Yes. Threat? Okay.

MS. K. SUZANNE BARBER: I like that.

MS. MELODI M. GATES: Hey, Joanne, this is Mel Gates. You might also be able to make that a little bit stronger if the initial statement there says the risk analysis should include assessing and so forth.

MS. JOANNE MCNABB: Yes, good. So if we -- so then it would be, "The risk analysis should include assessing the nature of the data, including its sensitivity," da-da-da, "and its usability. Other factors to consider include the nature of the data subjects and their vulnerability to harm, and the nature of the threat."

MS. SARAH MORROW: But then that sentence -- I'm sorry. This is Sarah Morrow again at Health and Human Services Commission (HHSC) in Texas.

So if we say that, then the next part -- clause doesn't kind of flow. "Other factors to consider include the nature of the data subjects and their vulnerability to harm

from the particular data breached." And then maybe after that parenthesis, say "and the threat -- the nature of the threat posed."

MS. JOANNE MCNABB: Yeah. That's actually where I -- that's where I was intending to put it, after the parenthetical expression. Sorry.

MS. SARAH MORROW: Perfect. Thank you.

MS. JOANNE MCNABB: I said "da-da da-da-da."

MS. SARAH MORROW: No, that's fine. Thank you.

MS. JOANNE MCNABB: Yeah. And the nature of the threat, I kind of think it's better to say "the nature of the threat," rather than "the nature of the threat posed" because we're kind of talking about the threateners, aren't we?

MS. SARAH MORROW: Sarah again. And agreed.

MS. JOANNE MCNABB: Yeah.

MR. RICHARD WICHMANN: Yeah.

MS. JOANNE MCNABB: Okay, good. So, so for the -- I'm writing this down as well and can send my version to you, Sandy. But for whoever is writing it down there.

MS. SANDRA TAYLOR: Okay. Thanks, Joanne.

MS. JOANNE MCNABB: In the top paragraph on page 3, one, two, three, four, fifth line where there's -- after the parenthesis following "harm," put a comma, and then it says "and the nature of the threat."

And then in the first sentence of that paragraph, the first line, "The risk analysis," change -- replace "would" with "should."

MS. SANDRA TAYLOR: Okay, Joanne. Thanks.

MS. JOANNE MCNABB: Okay. Good. Thank you, everybody.

Then we discussed briefly as to the timing issue, which was one of the -- part of that question that it's all this has to happen fast because you're always balancing the need for speed with the need for accuracy. And we've proposed that in considering how to get that balance that you should again look at issues such as has the breach already become public? So there's potentially misinformation out there.

And does it propose -- does it pose a risk of imminent harm and as well as the scope of the breach. How many -- oh, how difficult it is to, in many cases, determine the scope of the breach. You don't want to over notify. But on the other hand, the facts will sometimes not ever become clear as to what the scope is. So it's a balance. We leave you with that. It's not always easy.

The second point, the second question that we addressed is about the notice itself, and we recommend that creating a template that you would then adapt for different incidents can help speed the process along. As to how to deliver -- the delivery mechanism, we recommend that first-class mail is generally preferred, that it's the most likely to get to the right place and the least likely to be overlooked.

In furtherance of it not being overlooked, we recommend that both the content and the envelope be designed to make it not look like junk mail, and we acknowledge that there are situations -- there are some situations where different delivery mechanisms are appropriate, such as in a situation where you have your normal mode of communication is email, which might be the case with employees or in the case of online account holders, that then an email would be an appropriate way to deliver the notice.

And we think -- yeah?

MR. ALLEN BRANDT: Joanne, before you go on, this is Allen Brandt. Do we want to be on record telling a whole industry in the U.S. that they're sending junk mail?

[Laughter.]

MS. JOANNE MCNABB: Ah --

MR. ALLEN BRANDT: Just call it advertising or something like that.

MS. JOANNE MCNABB: Sure. We could say that. And we speak more to that issue as we go on here of how to make it more recognizable and effective, too.

We acknowledge that there are cases where, because of the size of the breach, for example, or you don't have contact information to notify directly that you then have to go to a Web site notification. And part of our -- one of our recommendations is that in such cases, the link to the notice on a Web site should be recognizable. The topic should be recognizable, so such as "security incident" or "personal data breach information." And that we also say that media alerts are necessary to let people know that there is a Web site notification.

Going back to --

MS. SHARON A. ANOLIK: Joanne? This is --

MS. JOANNE MCNABB: Yeah?

MS. SHARON A. ANOLIK: Hi, Joanne. This is Sharon Anolik.

MS. JOANNE MCNABB: Hi.

MS. SHARON A. ANOLIK: I had -- hello -- a question or a comment about this paragraph, the one that begins "When postal or email addresses for those affected are not available --"

MS. JOANNE MCNABB: Mm-hmm.

MS. SHARON A. ANOLIK: The way it's written, it sounds like that notice -- notice on a Web site should only occur if postal or email addresses are not available or the number is so large as to make emailing unfeasible. But I think, especially in large-scale breaches, I see more and more where Web site notices are done in addition, as part of a way of verifying the credibility of providing for the reliable proclamation that notice that one has received or press about something is real.

And so I wonder if there is an opportunity to maybe not require it, but at least note that it's a good practice?

MS. JOANNE MCNABB: Yes, absolutely. And in fact, we do mention that in answering the last questions about providing additional support. So, so on page 5.

MS. SHARON A. ANOLIK: Right. I saw that. I felt like that was focused more on the additional facts as things became available. But even to have the initial notice --

MS. JOANNE MCNABB: To supplement it.

MS. SHARON A. ANOLIK: -- right from the beginning, before additional facts are available, can be helpful in large-scale breaches.

MS. JOANNE MCNABB: Mm-hmm, mm-hmm. But it still would be a supplement.

MS. SHARON A. ANOLIK: Correct.

MS. JOANNE MCNABB: You don't want to give the idea here this would be instead because --

MS. SHARON A. ANOLIK: Correct.

MS. JOANNE MCNABB: -- our recommendation said, you know, preferred way is direct individual notice by first-class mail, secondarily email in some cases.

MS. SHARON A. ANOLIK: Absolutely. That is the preferable way. I just wouldn't want someone to walk away from this and think then that the only time it would make sense to have a Web site notice -- notice on a Web site would be if one of those two things in that first sentence are the case. I mean, this can be a supplement in addition to first-class mail.

MS. JOANNE MCNABB: So you'd want to put a sentence in here mentioning that supplemental role --

MS. SHARON A. ANOLIK: Right. At the end of that paragraph perhaps that even if postal or email addresses are available, providing the notice simultaneously on -- on the Web site can help to verify credibility of the notice or verify the information. You can play with the words, but that's the content.

MS. JOANNE MCNABB: Yeah. How about adding that qualification or that elaboration about the verifying role of a Web site notice to the end because it's -- to the end paragraph where we talk about supplemental use? Because it is still supplemental.

So on page 5, under number 4, that first paragraph ends with "A Web site can be used to provide updated information." Da-da-da. "Web site notice also -- can also serve to verify the authenticity of written notices."

MS. SHARON A. ANOLIK: Sure. Sure.

MS. JOANNE MCNABB: That sort of seems like the place for it. Web site -- so I'm putting it at the end of the paragraph where you've got the green arrow pointing right now. And so it says, "Web site notice can also verify and -- can also be used to verify," I guess.

MS. SHARON A. ANOLIK: Right.

MS. JOANNE MCNABB: "Used to verify the authenticity of a written notice." Does that do it?

MS. SHARON A. ANOLIK: Yep, thank you. Then I have one small typo.

MS. JOANNE MCNABB: Okay, good.

MS. SHARON A. ANOLIK: Let me find it here. On page 4 in the second full paragraph, the one that begins with "It is important."

MS. JOANNE MCNABB: Uh-huh.

MS. SHARON A. ANOLIK: The sentence, "A fraud alert does not provide any protection against someone using a stolen credit card."

MS. JOANNE MCNABB: Oh, you're right. Yes.

MS. SHARON A. ANOLIK: Thank you.

MS. JOANNE MCNABB: Thank you. Did you get that back there at the mothership?

MS. SANDRA TAYLOR: Hey, Joanne. This is Sandy. I do have that. Can you -- can you just clarify for me? So we're under 4, providing additional support for affected individuals, and we're at the end of the first paragraph. Is that correct?

MS. JOANNE MCNABB: Yes.

MS. SANDRA TAYLOR: Okay. Can you repeat what she --

MS. JOANNE MCNABB: Yes.

MS. SANDRA TAYLOR: Okay, I'm ready.

MS. JOANNE MCNABB: "Web site notice can also be used to verify the authenticity --"

MS. SANDRA TAYLOR: Okay.

MS. JOANNE MCNABB: "-- of a written notice."

MS. SANDRA TAYLOR: Got it. Okay. Thank you.

MS. JOANNE MCNABB: So back to page 3. We state that the notice should be in plain language, no jargon. And when the data subjects are known to have different languages, then the notice should be provided in different languages and should also be provided in forms that make it available to people with visual or auditory impairments.

The format should make it easy to read, including using headers to highlight the key sections. For example, and as it happens, these headers are part of California law now. But it's sort of logical stuff. What happened? What information was involved? What DHS is doing to help. What you can do. For more information.

And the contents should be focused on the information that the recipients need to

understand what happened and what they need to do now. And we point out that a lot of extraneous information can obscure the essential points and also contribute to the difficulty that people can have in understanding that this is a breach notice and not some other kind of communication.

On the question of source as who issues the notice, we recognize that there are situations where a third-party vendor, not DHS itself, it's the third-party vendor whose system is breached when they're operating on behalf of DHS. Our recommendation is the notice comes from whoever it is that the data subjects will recognize, that it's complicated for them to -- confusing to get a notice from some third party that they've never heard of unless they know that they have a relationship with that third party.

So the notice should be presented as from whoever that has the most direct relationship with the recipients of the notice and should be signed by a pretty high-level person in that entity.

MS. C.M. TOKË VANDERVOORT: Hi, this is Tokë Vandervoort. Don't we have some sort of a perception issue with, you know, I think we've all gotten the bogus IRS emails and phone calls and things like that. Do we have a concern about making sure that the person receiving this knows the authenticity and can trust that authenticity?

I mean, I know that if I got something like that, I would likely disregard it because I've been so conditioned to the other ones.

MS. JOANNE MCNABB: If you got something --

MS. C.M. TOKË VANDERVOORT: Especially if -- especially if there's a link that I'm being asked to click through and especially if that link is going to ask me for any information so that I can confirm what happened to me.

MS. JOANNE MCNABB: So, many of our recommendations about how to format and package the notice are designed to create a -- to reinforce its authenticity as well as the newly emphasized point about putting a Web site notice, Web site information about it as well to help authenticate it.

So what -- what would you suggest?

[Pause.]

MS. JOANNE MCNABB: Hello? Are we still here?

MS. C.M. TOKË VANDERVOORT: No, I'm sorry. I didn't have you off of mute. My apologies. You know, I know that people always have their antenna up, and the prevailing advice is to have your antenna up about those kinds of things. And

if that's how someone's information was compromised -- because someone mentioned phishing earlier, for example -- it's a fine line. I get it.

But I don't -- I don't know whether the -- you know, the high-ranking title of the individual is the thing that makes it grab someone's attention. I mean, this is very much a social question as much as it is sort of a language question. I know from, you know, what we hear and read and advise people that we would probably tell them, you know, listen, if you're clicking through for information, that's great.

And if further instruction was there, you know, "Please log in to your account" or "Please check with your -- you know, your credit providers" or put a freeze or do whatever, giving people additional steps that they can take that don't have them leaving that interaction with the sense that they've been lured into giving information.

MS. JOANNE MCNABB: Mm-hmm.

MS. C.M. TOKË VANDERVOORT: Yeah. As opposed to resources for figuring it out on their own. And maybe even explaining it that way as, you know, listen, we don't want you to feel like you're being lured into this information. So we encourage you to check on your own accounts and your own information, you know? I'm not really sure how to go about it, but I know that I would have my antenna up if I received a notification like this, and it went a little too far.

MS. JOANNE MCNABB: You haven't received one?

MS. C.M. TOKË VANDERVOORT: Yeah. No, no, no. I've received plenty of them. But even from Homeland Security is my point.

MS. JOANNE MCNABB: Oh, oh, oh. Ah.

MS. C.M. TOKË VANDERVOORT: And maybe from Homeland Security, it would be like those ones that are, you know, tantamount to the IRS. But you know, the advice that the IRS would dispense is we will never ask you for that information, to give it to us.

MS. JOANNE MCNABB: Right.

MS. C.M. TOKË VANDERVOORT: We already know it, you know? And so we don't need to ask you to confirm it or to log into your account or something like that. So don't fall for that.

I just feel like that same advice would probably be followed by people who are aware of that advice.

MS. JOANNE MCNABB: Right.

MS. C.M. TOKË VANDERVOORT: And that people -- and that if a notification like this got picked up by bad actors that, you know, someone could repackage a notification that looks very much like this one and lure people into making some mistakes. There's that sensitivity to it.

I realize you're taking all the steps to put it in there. I'm not really sure -- I don't know. I'm not -- I'm not reacting to this like that's being addressed. You're making a lot of points about how to work around that and make it appear authentic, but I just -- I feel like it needs to also make people feel safe --

MS. JOANNE MCNABB: That advice is --

MS. C.M. TOKË VANDERVOORT: -- if there's any interaction from an email like that.

MS. JOANNE MCNABB: Yeah. So, so it's the fact that it would be DHS that -- so in my experience, most notices, the only place where they would have, if they do at all, a "click on this" would be to -- unless it's your own online account, and you're told to go in and change your passwords. But in general, it would be if that's a means to sign up for some kind of mitigation product.

And I don't know if that's by phone usually or whatever. I'm trying to think of the information in a notice usually isn't saying send -- so now send your Social Security number here. It's not usually doing the thing that a phishing email or letter would do. It's not making that request. It's putting out information.

MS. C.M. TOKË VANDERVOORT: Yeah. That's what I'm getting at, but the suggestion in here about, you know, links through and things like that, I just think people need to be cautioned about it.

MS. JOANNE MCNABB: There could be a mention about language --

MS. C.M. TOKË VANDERVOORT: And maybe that's one of those things that you say, look, we're never going to ask for your information that way, but we encourage you to go check on your information this way. You know, in terms of just how to frame it to give people that assurance.

MS. JOANNE MCNABB: Mm-hmm. Anybody have an idea about that?

MS. C.M. TOKË VANDERVOORT: It could be as simple as that. It could be as simple as a very just sort of, you know, person-to-person kind of, you know, piece of advice. Like this is where you can get more information about this breach. We encourage you to check on your own accounts.

You know, we're not -- we, DHS, like other Government entities, are not going to

ask you to log in and give your information. That should be a red flag to you, right? But here's how you should go and check on your own information. Just part of the narrative is what I'm getting at.

MS. SARAH MORROW: Excuse me. This is Sarah Morrow. Isn't that covered in the last -- answering the last question? Where you have resources and suggestions. Because when you receive a large breach notification, it's going to have a Web site for you to go so you can sign up for credit monitoring and for how many years you get it.

And so that part gets confusing if you say we will never ask for this. Because in a civilian's mind, that's like but you are because they have to give that information to the credit monitoring agency so that they can actually monitor the Social Security number. So I just -- I wonder whether that might be a little confusing, and that's why I would say put it down at the bottom with other resources.

MS. C.M. TOKË VANDERVOORT: Yeah, that's a good place for it. Give it a call out.

MS. JOANNE MCNABB: Why don't you think about what might be added to that paragraph as we work our way to it, and let's see where we are then?

I take the point. I'm just thinking that in general a breach letter isn't asking -- except in that one case, isn't asking for information. But it's a point still. So can we talk about that in just a minute?

MS. SARAH MORROW: Oh, absolutely, yeah. I appreciate it, and it was no -- it was no offer of criticism. It was just one of those things --

MS. JOANNE MCNABB: No, no. I think it's a point.

So then we addressed the question about over notification, and we note that the new OMB, Office of Management and Budget, memo on breach response mentions it also that agencies should balance the need for transparency with concerns about over notifying. And we note that the Federal Trade Commission (FTC) expressed concern about that in their comments on the broadband privacy rule from the Federal Communications Commission (FCC), and we also cite some research that kind of suggests that this over notification leading to disregarding may not be occurring.

Javelin Strategy and Research that does this ongoing research on identity theft and data breach, and it's consumer research, and they found that during a period when people were getting more notices that at the same time -- or more people were getting notices at the same time, more people were taking -- indicated that they felt that you need to take action when you got a -- when you got a notice.

So it's you can't say that there isn't the possibility of over notification, but people do seem to be taking data breach notices seriously, and we ultimately concluded that it's really up to the individual to decide how they're going to react to a notice, that we shouldn't be second-guessing for them and deciding to not notify because we're afraid they won't -- that they've gotten enough notices. And point out that reducing the likelihood that people become desensitized can be -- you can help -- we can reduce the likelihood that they'll become desensitized by using good language and format that make it easier to understand what the notice is and what it is that they're supposed to do about it so that they can take, make -- assess their own risk and take appropriate action.

And then the final question that we addressed is what additional support should be offered, and here is where we -- oh, I have two little edits here. Typo, one of them.

So in the first sentence, "No matter how clearly they are written, most --" delete "most" -- "breach notices should be supplemented with additional sources of information and assistance." So delete "most" in that sentence.

And then in the next sentence, "A call center," the last two words "is essential" should be deleted. That's a typo. So we say that --

MS. SANDRA TAYLOR: Got it.

MS. JOANNE MCNABB: Yes?

MS. SANDRA TAYLOR: I got it. Thanks, Joanne.

MS. JOANNE MCNABB: Okay. So the point is that even the perfect notice is going to generate further questions in the minds of at least some people, and so a call center that is trained and prepared to answer questions is essential.

And on the -- the necessity of having a well-prepared call center is also a factor in balancing the timing, that to issue a notice before you're prepared to handle the calls can create problems for people. At the same time, other factors may push you toward notifying rapidly or just consider the need to have a well-prepared call center in looking at your timing.

Then we talked about the role of a Web site that it can keep -- it can supplement a notice, a written notice by providing additional information as it becomes available, and then now we have added this section, the point about the Web site can also help individuals to verify the authenticity of the notice. So we put that in.

In discussing the mitigation products, the point that we made is that they need to be appropriate to the nature of the incident and the nature of the data. So, for

example, in the case of a breach of credit card account numbers, a credit monitoring product does not provide any assistance that's beneficial in situations where Social Security numbers had been breached. So that's our recommendation about a mitigation product.

So here is where we might add something about ensuring that -- hmm, that -- maybe it isn't here. That the notice not -- I don't know. What would we want to say here on the point about it not looking like a phishing and not being an opportunity for phishing?

MS. K. SUZANNE BARBER: I think in email, that's tough. Because the analogy is the IRS one. I mean, the IRS is pretty clear about that, that they don't send notifications via social media or electronically, right?

MS. JOANNE MCNABB: Mm-hmm.

MS. K. SUZANNE BARBER: So that already makes it a little harder.

MS. MELODI M. GATES: Joanne, this is -- this is Mel. I'm wondering if maybe, since we're trying to give broad advice here, though, you could just add a sentence into that paragraph. You know, something to the effect of "However, any communication regarding mitigation products or other services should be done in a manner that is mindful of the recipient's perception and potential phishing risk." Or, you know, just a broad statement like that --

MS. JOANNE MCNABB: Uh-huh. I like that.

MS. MELODI M. GATES: -- to remind people to balance the two things.

MS. JOANNE MCNABB: Yeah.

MR. ALLEN BRANDT: This is Allen. Do we want to send people back to the Web site that says before you provide information, check our Web site for authenticity or check the Department's Web site?

MS. SARAH MORROW: Allen, this is Sarah. I was just thinking about that myself. At the end of that paragraph where it says a Web site can also blah-blah-blah, might we not add a sentence that says this is also another opportunity to remind individuals that we don't ask for that kind of information and how they could check the veracity of the situation.

MS. C.M. TOKË VANDERVOORT: The IRS actually has its own Web page that does exactly that. I think that's a really good suggestion.

MR. ALLEN BRANDT: Yeah, they do.

MS. JOANNE MCNABB: So, so let's have the sentence that says this is also another opportunity to da-da-da. What was the da-da-da?

[Laughter.]

MS. SARAH MORROW: This is also another opportunity to -- good Lord, I don't even know what I said -- to confirm the veracity or the authenticity of the situation without asking for further information, without asking for you to input your personal, private information.

MS. JOANNE MCNABB: I'm kind of liking whoever had said earlier the point about any communication about mitigation products should be structured -- I'm kind of liking that one as being a little more direct. Any communication about mitigation products should what?

MS. MELODI M. GATES: Hey, Joanne, this is Mel. I think I was suggesting that earlier, and my suggestion was any communication should be structured in a manner to balance the notice with not creating phishing risk.

MS. JOANNE MCNABB: Oh, I see.

MR. ALLEN BRANDT: Or not creating additional risk.

MS. MELODI M. GATES: Right, right. I mean, I'm just concerned here that if we try to get too prescriptive in this --

MS. JOANNE MCNABB: Uh-huh.

MS. MELODI M. GATES: -- that it's going to start reading like a cookbook, and I mean, we've all been through this, right? The cookbooks don't work, and they end up with unintended consequences.

FEMALE SPEAKER: -- to provide comment. It just would be listed, yes.

MS. JOANNE MCNABB: Mm-hmm. Good point. Any communication about mitigation products should be structured to --

MS. MELODI M. GATES: Yeah.

MS. JOANNE MCNABB: -- to reduce any instance of phishing?

FEMALE SPEAKER: No. That's absolutely right. And you know, obviously, we'll have the wherewithal to do that if we need to. So that's fine.

MS. JOANNE MCNABB: Okay. How about this? Any communication about mitigation products should be structured to avoid creating --

FEMALE SPEAKER: This is embarrassing us. I mean, do we look --

MS. JOANNE MCNABB: -- phishing risk, phishing risk? A risk of phishing? No, I like phishing risk. Any communication about mitigation products should be structured to avoid creating phishing risk.

What do you think, Lisa?

MS. LISA J. SOTTO: I agree --

MS. JOANNE MCNABB: Queen of breaches.

MS. LISA J. SOTTO: Yeah, I agree with the comment of not making this too prescriptive. That's my overarching concern because I think there's little chance that in the heat of the moment anybody can follow a cookbook.

MS. JOANNE MCNABB: Mm-hmm.

MS. LISA J. SOTTO: So I think -- I think I would frame it in terms of consider how to -- what's the rest of it. Just make it a consideration instead of a "should."

MS. DEBBIE MATTIES: And this is Debbie Matties. We're not trying to avoid a phishing risk. We're trying to avoid someone thinking it's a phishing risk.

MS. JOANNE MCNABB: Yeah, exactly.

MS. LISA J. SOTTO: Right.

MS. JOANNE MCNABB: Consider how to structure --

MS. LISA J. SOTTO: But that sometimes it's hard to do it.

MS. JOANNE MCNABB: Yeah.

FEMALE SPEAKER: Well, and it's not just phishing. It's any kind of social engineering as well. So --

MS. JOANNE MCNABB: Yeah. How about "Consider social engineering risks in your communications about mitigation products."

MS. LISA J. SOTTO: Perfect.

MS. SARAH MORROW: Wahoo. I like that.

FEMALE SPEAKER: That's great.

MS. JOANNE MCNABB: Okay. "Consider social engineering risks," plural, "in your communications --" we can say "you," can't we? I can't remember if we ever use second person.

MR. ALLEN BRANDT: Or "the communication."

MS. JOANNE MCNABB: "In the communication about mitigation products."

MS. SANDRA TAYLOR: Okay, Joanne, this is Sandy. "Consider social engineering risks in the communication about mitigation products."

MS. JOANNE MCNABB: Right. And that goes at the end of the first paragraph under number 4. Or no, no, let's put it at the end of -- at the very end, where we're talking about mitigation products. So it's the last sentence.

MS. SANDRA TAYLOR: Got it. Okay.

MR. ALLEN BRANDT: Now do you want to add something there, Joanne, about put a notice on the -- you can, you know, put a notice on the Web site that consumers can use to check?

MS. JOANNE MCNABB: I think we kind of covered that in the addition to the previous paragraph. "Web site notice can also be used to verify the authenticity of a risk."

MR. ALLEN BRANDT: Okay. Okay, just leave it there.

MS. SANDRA TAYLOR: Hey, excuse me one second, guys. I'm going to ask the operator to -- Marjorie Weinberger is muted. She's one of our members. Can you please unmute all the lines so they can have an opportunity to talk, please?

OPERATOR: Yes, ma'am. She did request to have her line muted because of background, and her mute wasn't working. So now her line is open.

MS. SANDRA TAYLOR: Okay. Thank you.

MS. MARJORIE S. WEINBERGER: Thank you very much. I apologize for being difficult. I've been muted in maybe something I was going to say.

I do want to back up just a moment on the communications discussion, where it began with communications should not be of a legal nature. Information that's being provided needs to meet accessibility standards, and I don't think we had enough language in there regarding the need to comply with Section 508, and we didn't offer a TTD -- excuse me, TTY line or fax.

So the idea is not just, you know, people who may have low vision or moderate vision or audio issues. We need to be more broad spectrum than accessibility. And so I was hoping we could add additional language on how to assist persons with disabilities in compliance with Section 508.

MS. JOANNE MCNABB: So you mean -- so right now you're talking about on page 3, the last little paragraph that starts on page 3 where it says visual or auditory? You want to elaborate there, or you want to put it at the end in the additional support?

MS. MARJORIE S. WEINBERGER: I was thinking putting it there because you mentioned how it should have a telephone number involved. It should be a TTD number or fax number.

MS. JOANNE MCNABB: There should be --

MS. MARJORIE S. WEINBERGER: And there should be some language in that paragraph indicating that all communications should comport with the requirements of Section 508 for persons with disabilities.

MS. JOANNE MCNABB: I'm -- I take the point. I think we can easily add a little. So now I'm on page 5 where we talk about the call center in multiple languages and -- and with some sort of reference there to TTD/TTY, whatever. But I mean, there are a lot of laws that DHS has to comply with as well as what we're saying here. I don't know that we need to suddenly pop up with Section 508. It seems sort of --

MS. MARJORIE S. WEINBERGER: Well, I mean, it is something that the Feds all are required to manage.

MS. JOANNE MCNABB: Yes.

MS. MARJORIE S. WEINBERGER: I mean, I don't mind if we don't do it. But we need to be more broad spectrum than how we address communications for persons with disabilities. It could include a videophone, a TTY line. But I don't think we should just limit it as it is because it's kind of a throw-away line as opposed to we really want to make sure that we have broad spectrumed our communication to reach all persons with disabilities.

MS. JOANNE MCNABB: So how about if we add -- so not -- on page 5 right after multiple language, how about if we add a sentence that says "Call center info should also be made available --" how can we say that simply?

MALE SPEAKER: How about just made available --

MS. MARJORIE S. WEINBERGER: And it's not just call center info. It has to do with the written notices as mentioned earlier in the document.

MS. JOANNE MCNABB: Oh, so it's there.

MS. MARJORIE S. WEINBERGER: Mm-hmm. I mean, in the call center, we have to make sure that the call center has either a videophone or a TTD line for people with disabilities. But in the written communications, you have to validate that it does not, you know, discriminate against persons with disabilities, and that has to do with pixelation and any use of images, whether it can be hovered over and language be on the image.

So even just a line that says that, you know, all written communications must be --

MS. JOANNE MCNABB: So on page 3 then, "The notice should be written in plain language --" da-da da-da-da.

MS. MARJORIE S. WEINBERGER: Yes.

MS. JOANNE MCNABB: It should be in languages other than English when the language is known, and the information should be available to people with disabilities?

MALE SPEAKER: Perfect. That's what I think.

MS. MARJORIE S. WEINBERGER: Yeah. And I think you want to say maximize accessibility, you know? Because disabilities is so broad. The whole point of it is to make sure that we maximize capacity of all persons to have accessible communication.

MR. RAY MILLS: I agree with that. This is Ray Mills from the Headquarters Office of the CIS Ombudsman. And having worked on Section 508 as well as the language accessibility policy for all of DHS, you can perhaps craft a sentence that determines or defines or describes accessibility per Executive Order 13166, which covers your languages, and then the appropriate executive order for persons with disability.

And if you put that up front, that way you can say everything that follows herein will adhere to these making the information accessible to, you know, the maximum amount of individuals. And as we all know, we face -- we do face resource constraints. So you would say that, you know, to the extent possible.

MS. JOANNE MCNABB: What about -- I'm still looking at the same paragraph about the notice should be written in plain language and changing people with disabilities instead of visual/auditory impairments. How about a footnote and put

all that stuff in the footnote?

MR. RAY MILLS: That would be fine. That way you could see what exactly you're referring to, which is making it available to everyone who has limited English proficiency as well as those who have different disabilities to have the information imparted to them as anybody else should reasonably expect.

MS. JOANNE MCNABB: What is the -- what do other committee members think about this?

MS. MELODI M. GATES: Joanne, this is Mel. Maybe to simplify that, you could just take that sentence and say it should be in languages other than English -- comma -- and the information should be communicated in a manner that maximizes accessibility. Then drop the footnote you were just talking about.

MS. JOANNE MCNABB: And the information should be communicated in a manner -- so that it makes it stronger even in the body. Manner --

MS. MARJORIE S. WEINBERGER: Actually, this is Marjorie, and I appreciate that. As a lawyer, I stick bad news in a footnote. So having it in the main body of the document I think is helpful.

MS. JOANNE MCNABB: Yeah. And so, so that sentence now, "The notice should be written in plain language." Oh, and the next sentence, "It should be in languages other than English when the recipients' language preferences are known, and the information should be --" Now we cross out what's written there now in that sentence. "Should be communicated in a manner that maximizes accessibility." Footnote.

And then who's got the footnote?

MR. RAY MILLS: Well, it could be maximizing accessibility per existing Federal statutes, and then you just plunk in your executive orders there. I know the one is 13166 for language accessibility, but I'm not sure of the one that would be the one that, of course, enunciates Section 508.

MS. JOANNE MCNABB: So who can provide that to us? I mean, not necessarily right this instant. Sandy, we -- Sandy or Lisa, we could vote on this, subject to getting that footnote nailed down, couldn't we?

MS. SANDRA TAYLOR: Yes.

MS. JOANNE MCNABB: Okay.

MS. LISA J. SOTTO: I think that's the right way to do it.

MS. JOANNE MCNABB: But who's going to nail -- who know -- who's going to be able to give us the proper citations?

MS. SANDRA TAYLOR: I can get it from our advisers here at the Department. This is Sandy.

MS. JOANNE MCNABB: Yeah, okay. So, so do we know where we are, how that sentence will read? "The information should be communicated in a manner that maximizes accessibility." Footnote.

MS. SANDRA TAYLOR: Per Federal statute. Didn't Ray say "per Federal statute," and then we're going to actually footnote the actual statutes? Isn't that correct?

MS. JOANNE MCNABB: Uh-huh. Is that what we want to do, everybody?

MS. MARJORIE S. WEINBERGER: I think that's appropriate.

MS. JOANNE MCNABB: Okay. Per Federal requirements probably, if we're going to count an executive order.

MS. DEBBIE MATTIES: This is Debbie Matties. If they're Federal requirements, is there a reason to put them in the document in the first place? Are we doing that with other Federal requirements? It feels like it's opening a door to a lot of potential --

MS. JOANNE MCNABB: That's kind of where I -- that was kind of the way I was looking at it, too. But I like -- I like making the point about communicated in a manner that maximizes accessibility. That's a nice policy statement.

MR. ALLEN BRANDT: I do, too. And it kind of reminds you in the heat of the moment that your call center needs to be compliant, or something like that.

MS. JOANNE MCNABB: Mm-hmm. How about we don't say "per Federal requirements," but we do footnote them?

MR. RAY MILLS: I think that works.

MS. MARJORIE S. WEINBERGER: I don't --

MS. JOANNE MCNABB: I mean, obviously, you've got to --

MS. MARJORIE S. WEINBERGER: I don't object to that.

MS. JOANNE MCNABB: There are lots of Federal requirements. We're not exempting DHS from any of them. So I'm back now to page 5 to the call center

place, where we've got to put a little something in there. Call center staff, multiple languages where appropriate, and --

MR. ALLEN BRANDT: Multiple languages and accessibility.

MS. JOANNE MCNABB: And should be accessible. Multiple languages --

MS. MARJORIE S. WEINBERGER: Multiple modes of accessibility, yeah.

MS. JOANNE MCNABB: Okay. And multiple modes of accessibility.

MS. MARJORIE S. WEINBERGER: Or methods to maximize accessibility.

MS. JOANNE MCNABB: It should be available in multiple languages where appropriate. Because it isn't always going to be appropriate. Where appropriate. And --

FEMALE SPEAKER: In multiple languages and using -- in multiple languages and methods. You could just make it simple.

MS. MARJORIE S. WEINBERGER: Do you want to reference the TTY line and videophone options, which are perhaps the most well-known used ones?

MR. ALLEN BRANDT: Something like including -- this is Allen -- "including, for example, TTY and video options, among others." Or something -- or just "including, for example."

MS. JOANNE MCNABB: Okay. Yeah. Include --

MS. SANDRA TAYLOR: Okay, everyone. Remember you have to announce yourself when speaking.

MR. ALLEN BRANDT: I got smacked. I heard you.

MS. SANDRA TAYLOR: Thanks.

MS. JOANNE MCNABB: So how about this? The call center -- "A call center with staff that has been appropriately trained should be available to answer questions in multiple languages where appropriate and should include TTY or other accessibility mechanisms."

MR. RAY MILLS: This is Ray Mills. I like that. It's very good.

MS. SARAH MORROW: Sarah Morrow. Yes. Wahoo, that sounds great.

MS. JOANNE MCNABB: Okay. So after "where appropriate," comma, "and

should include TTY or other accessibility mechanisms."

DR. CHARLES PALMER: Charles Palmer here. Quick question.

I've been listening to all this, and not being an attorney, maybe this is the wrong thing. But surely, this is stated clearly how all Government paperwork should be handled in announcements. Are we re-creating something here? Can we not, as we do in the geekland, just point at National Institute of Standards and Technology (NIST) and say do what they said, some standard directive? Or do we have to put it here?

MS. MARJORIE S. WEINBERGER: Hi, this is Margie Weinberger. And coming from a State that is painfully eking out its accessibility requirements, I think it's called for here as we are reaching out potentially to broad communities with information as essential as breach. So I would -- I think we'd be remiss not to use the opportunity to drive it home.

DR. CHARLES PALMER: I'm perfect -- this is Charles again. I'm perfectly fine with that. It just seems like we're going through something that there's going to be 50-something versions of it or more, and how will we know that this is going to be sufficient?

But again, like I said, I just wanted to raise the question because I've been sitting here stewing. So I defer to the attorneys, as always.

MS. MARJORIE S. WEINBERGER: This is Margie. That's always a mistake. I appreciate that.

MS. JOANNE MCNABB: I --

MS. LISA J. SOTTO: But I think that's -- I think that's a really important point because, I mean, I can say I don't -- this is Lisa. I don't know anything about this area, and I would hate to have any conflicting or even overlapping language in here if there's something else we can point to.

MR. RAY MILLS: And this is Ray Mills again. Well, without mentioning it, then you do perhaps open up a different set of floodgates when it is sort of under the microscope or floodlights of public review. And as long as it's there to begin with and we don't really get too much into the weeds and we just refer to it, then individuals can go to that and see that it is a well thought out thing that the Federal Government is trying to make it as inclusive and all encompassing as possible.

You know, we don't have to get into the weeds of defining it, but we do have to at least mention it. That way, they know that we've done our due diligence. We're not just putting something out here that isn't trying to include everyone. Or trying

to exclude anyone, I should say.

MS. JOANNE MCNABB: Does anybody think that we are creating a problem by adding this language?

MR. ALLEN BRANDT: This is Allen. I don't think so.

MS. LISA J. SOTTO: What do the experts think? Who are the folks who understand this area? I am not one.

MS. JOANNE MCNABB: Ditto.

MS. MARJORIE S. WEINBERGER: Well, this is becoming a daily issue in Massachusetts in our communications with the public, and we make sure our official notices identify that we will make reasonable accommodations for persons with disabilities and maximize accessibility opportunities.

MS. JOANNE MCNABB: So thinking as a policy, it's kind of good to mention this, as somebody said, in the -- to have it up there in your mind in the heat of the breach, in the fog of breach.

MS. LISA J. SOTTO: I agree with that. I just want to make sure that we're not stepping on anything else that's out there.

MS. JOANNE MCNABB: Right. Yep. So assuming we're leaving it in as is and that the footnote is to be developed, that's it. Further discussion? What's the next step?

[Pause.]

MS. SANDRA TAYLOR: Lisa?

MS. LISA J. SOTTO: Well, I think once we finalize this, I think we can -- I think we're done. Sandy, do we need any further public notice?

MS. SANDRA TAYLOR: Well, we need to send it -- I mean, we need to make the changes, identify, and we need to make sure all of the members are in agreement with the changes that we're going to make. And so I guess I think we need to vote on this document as is with the changes, and then we can just go from there. We can adopt the -- we can adopt the report as is.

MS. LISA J. SOTTO: Okay.

Agenda Item: Public Comments

MS. SANDRA TAYLOR: Do we have any questions from any members of the

public? I didn't get any. So I'm going to open it up -- open it up now to members of the public. Do you have any questions, issues, and/or concerns?

MS. LISA J. SOTTO: And I'll just ask the committee members if anybody thinks we need another meeting to discuss the next draft, or if you think the substance has been fleshed out sufficiently here so that the rest is really religious drafting?

MS. SARAH MORROW: This is Sarah Morrow. I think we're good.

MS. LISA J. SOTTO: Okay.

Agenda Item: Committee Vote on Policy Subcommittee Recommendations – Data Breach Notification

MR. ALLEN BRANDT: This is Allen. I'll make the formal motion to accept the document with the changes we discussed today.

MS. SANDRA TAYLOR: Okay. Can I get my committee members, is everyone in agreement?

[Response.]

MS. LISA J. SOTTO: I think we have agreement, yeah. Do we have -- let me ask this. Otherwise, we can assume consensus. Does anybody disagree?

MS. SANDRA TAYLOR: Yes.

[No response.]

MS. LISA J. SOTTO: Okay. Silence is -- so there we are. We have consensus around the paper.

MS. SANDRA TAYLOR: Yes. Great. And I think that's it. We didn't have any -- any questions from members of the public. I'll make the changes. I'll work with Joanne and get this finalized and get it sent around to all of our members.

MS. LISA J. SOTTO: And I'm happy to look at changes as well, any of the revisions, just to make sure they're consistent.

MS. JOANNE MCNABB: So are we going to vote?

MS. SANDRA TAYLOR: Yes, let's vote. Well, we just asked -- we just asked --

MS. LISA J. SOTTO: Yeah, so we just had consensus. Is consensus sufficient?

MS. JOANNE MCNABB: We didn't have to do more than that, huh? Okay.

MS. LISA J. SOTTO: I don't know. Sandy?

MS. SANDRA TAYLOR: Yeah, we didn't get any objections from any of our members, and everyone is on the phone, with the exception of Julie Park.

MS. JULIE PARK: I'm on the phone. I'm here.

MS. SANDRA TAYLOR: Oh, okay. Good.

MS. JULIE PARK: I have no objections.

Agenda Item: Meeting Adjourned

MS. SANDRA TAYLOR: Okay. So, with that, I think the report has been adopted.

MS. LISA J. SOTTO: Done.

MS. SANDRA TAYLOR: This is Sandy, by the way. We'll make the changes. I'll get it sent around to all of our members, and with that, I think we can conclude our meeting.

MS. LISA J. SOTTO: Thank you very much to all.

MS. SANDRA TAYLOR: Thank you.

MS. LISA J. SOTTO: And thanks for your time this morning. Thank you, bye.

[Whereupon, at 11:20 a.m., the meeting was adjourned.]