

[REDACTED]

From: HUSTINX Peter
Sent: 23 January 2012 16:10
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Meeting request - U.S. Ambassador [REDACTED]

OK for us.

From: [REDACTED]@state.gov]
Sent: 23 January 2012 15:12
To: HUSTINX Peter
Cc: [REDACTED]
Subject: FW: Meeting request - U.S. Ambassador [REDACTED]

Dear Mr. Hustinx,

Thank you for your availability and flexibility to meet with Ambassador [REDACTED]

We would be very pleased to schedule the meeting for Thursday at 10.45-11.15 at the EDPS offices if this works for you.

I will accompany the Ambassador for his meeting. Your office is welcome to contact me should further information be required.

With thanks and best regards,

[REDACTED]

This email is UNCLASSIFIED.

From: HUSTINX Peter [mailto:peter.hustinx@edps.europa.eu]
Sent: Monday, January 23, 2012 1:19 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Meeting request - U.S. Ambassador [REDACTED]

Dear Mr [REDACTED]

Time will be very limited on Thursday 26 January, but a brief meeting (30 min) somewhere between 10.00 and 12.00 would be feasible. I hope this works for Ambassador [REDACTED]. I will be travelling to Berlin by early afternoon.

Please let me know which time we should block in the agenda.

Best regards,

Peter Hustinx

European Data Protection Supervisor (EDPS)
Contrôleur Européen de la Protection des Données (CEPD)
Mail: Rue Wiertz 60 - MO 63
B-1047 Brussels

Office: Rue Montoyer 63, 6th floor
Tel: + 32-2-2831900
Fax: + 32-2-2831950
Email: edps@edps.europa.eu
Website: www.edps.europa.eu

From: [REDACTED]@state.gov]
Sent: 20 January 2012 11:06
To: European Data Protection Supervisor
Cc: [REDACTED]
Subject: Meeting request - U.S. Ambassador [REDACTED]

Dear Mr. Hustinx,

The U.S. [REDACTED], Ambassador [REDACTED], will be in Brussels for a short visit on January 26.

In view of your leadership in the European debate on data protection dossiers, Ambassador [REDACTED] would very much like to meet with you to discuss the forthcoming review of the EU Data Protection legislation.

Regrettably, Ambassador [REDACTED]'s visit is limited to January 26 only. Your office is welcome to propose a time that might work best and of course to contact me for any further details.

With thanks and best regards,

[REDACTED]

[REDACTED]

U.S. Mission to the EU
Rue [REDACTED], [REDACTED] Brussels
T: +32 [REDACTED]
M: +32 [REDACTED]
E: [REDACTED]@state.gov

This email is UNCLASSIFIED.

[REDACTED]

From: [REDACTED]
Sent: 20 January 2012 17:45
To: HUSTINX Peter
Cc: [REDACTED]; [REDACTED]; [REDACTED]
Subject: European-American Business Council: Meeting Request for 6-9 February
Attachments: EABC Overview - 2011 December 20.doc; EABC Member Companies - 2012 January 21.doc

Dear Mr. Hustinx,

I'm writing to request an appointment with you for senior EABC member company executives and myself in the February 6-9 period. We'd like to discuss the EU Data Protection Framework and its implications for Trans-Atlantic and global commerce. [REDACTED], Oracle's [REDACTED] and EABC Data Governance Group US [REDACTED] suggested that we ask to see you on this issue.

The European-American Business Council is the largest Trans-Atlantic business association. We represent 70+ US, Canadian and EU-based global companies. Please find attached the EABC Membership, as well as the EABC Overview.

Our group's current availability on 6-9 February is:

- 6 February from 14:00-16:00 CET
- 7 February from 10:30-18:00 CET
- 8 February from 9:00-12:00 CET
- 9 February from 15:00 – 18:00 CET

Our group will include the following executives:

- [REDACTED], [REDACTED], Oracle
- [REDACTED], [REDACTED], Research in Motion
- [REDACTED], [REDACTED], Deutsche Post DHL
- [REDACTED], [REDACTED], European-American Business Council
- [REDACTED], [REDACTED], European-American Business Council

Thank you for your consideration of this request. Please let us know if you can see us that week.

Kind regards,



[Redacted]

European-American Business Council

EABC [Redacted]

[Redacted]

WDC: [Redacted]

www.eabc.org



European-American Business Council

“Investment ~ Innovation ~ Integration”

EABC Overview

The European-American relationship is the most important commercial partnership in the world. With 11% of the world's people, the Atlantic market produces 50%+ of the world's GDP, trade and capital flows. Trans-Atlantic investment, innovation and trade foster prosperity across the Atlantic and around the world. The EABC is committed to fortifying EU-US economic investment, innovation, regulatory integration and competitiveness through its Atlantic Agenda and Programs. EABC's Atlantic Agenda includes issues before EU, EFTA, US and Canadian governments within a 'horizontal' policy model.

EABC History

The EABC was chartered in 1989 as the European Community Chamber of Commerce in the United States. On June 2, 1990 the EABC went public in New York and Washington as an independent business association wholly funded by its member companies. Founding Co-Chairs were Gerrit Jeelof, Chairman, Philips North America and John Bryan, Chairman, Sara Lee. Founding Members were Akzo Nobel, BASF, Bowater, BP, Enimont, Fragomen Del Ray, IBM, ICI, ING, Lazard Freres, Philips, PwC, Sara Lee, Siegel & Gale and Xerox - 9 European and 6 American-based firms. Today membership stands at 76. In 1997 the ECCC was renamed the European-American Business Council. The EABC is recognized as the official European Business Organization in America by the European Commission. With new leadership in 2003, the EABC expanded from a Washington-centric to a truly Trans-Atlantic voice for business. EABC's Brussels Office opened in 2005, and in 2010 it expanded its policy work to Canada.

EABC Mission

The 1990 ECCC Charter states "To support unrestricted trade and investment between the US and the EC, promote a healthy, open and productive business environment between the two regions... and provide a platform for discussion and exchange of ideas for business and government leaders in Europe and in the United States..." EABC's mission today remains the same, with expansion of our policy work to include EFTA nations and Canada. We promote a "win-win" EABC Policy Agenda with a central focus on Trans-Atlantic commercial regulatory and policy cooperation. EABC has forged policy alliances with numerous business associations which are members of the EABC Alliance Council. EABC company business models are "horizontal" in nature, reflecting the globalization of markets, technologies and business alliances. Sovereign governments are naturally "vertical" in structure. 21st Century business-government relations must pursue "horizontal public policies" to match global challenges and opportunities of the future. This reality lies at the heart of the EABC business model and mission.

EABC Canada

In 2010 the EABC expanded its Policy Groups & Programs work to active engagement with Canadian government officials and industry executives. This has met with solid success. In 2011 the Canadian flag was added to the EABC logo. We plan to significantly enhance our Canadian involvement in 2012.

EABC Board & Leadership

The US Chair of the EABC Board is the Hon. Stuart Eizenstat, former US Ambassador to the EU. The European Chair of the EABC Board is the Hon. Hugo Paemen, former EU Ambassador to the US. In 2012 we plan to name our first Canadian Chair. The EABC Board includes senior executives from 27 member companies and meets in semi-annual Trans-Atlantic conference calls.

EABC Staff

Michael Maibach was named EABC President & CEO in 2003. From 1983 - 2001 he was Vice President, Global Government Affairs, Intel Corporation. From 1976 - 1983 he was Government Affairs Manager, Caterpillar. Laura Reidy is Program Director. Justine Korwek is Brussels Director. Alex Propes & Ashley Chase are Policy Managers. Jessica Jones is Operations Manager. Contact: Jessica@eabc.org 12/20/11

Washington & Brussels ~ www.EABC.org



European-American
Business Council

US Based
EU Based
Canada Based
71 Companies

EABC Membership 2012

Agfa Healthcare	Deloitte	Nokia
Albemarle	Deutsche Post DHL	OMV
Alexion	Deutsche Telekom	Optimos
Aliaxis	DHL USA	Oracle
Amgen	eBay	PayPal
Apple	Ericsson	Pfizer
Applied Materials	Ernst & Young	Philips Electronics
AstraZeneca	First Data	PwC
AT&T	Grant Thornton	Qualcomm
Autodesk	Hogan Lovells	RIM
Bayer	IBM	SAP
BDO	Ingersoll Rand	Statoil
Biogen Idec	Intel	Telecom Italia
Boehringer Ingelheim	IPEX	Telefonica
BP	Johnson & Johnson	Texas Instruments
BT	Kodak	TE Connectivity
CA Technologies	KPMG	Underwriters Laboratories
Chrysler	Kreab Gavin Anderson	Unilever
Cisco Systems	Lilly	US Steel
Cognizant	LOTOS	Verisign
Covidien	McAfee	Verizon
Covington & Burling	Medco	Visa
Cubist	Microsoft	Vodafone
Daimler	NCR	Xerox

[REDACTED]

From: HUSTINX Peter
Sent: 25 January 2012 15:38
To: [REDACTED]
Subject: RE: European-American Business Council: Meeting Request for 6-9 February

Dear Mr [REDACTED],

OK for **Thursday 9 February at 17.00-18.00 CET.**

We will inform the guards at the reception of our European Parliament owned office building at Rue Montoyer 63. Registration of your delegation of six should not take more than 5 minutes.

Kind regards,

Peter Hustinx

European Data Protection Supervisor (EDPS)
Contrôleur Européen de la Protection des Données (CEPD)
Mail: Rue Wiertz 60 - MO 63
B-1047 Brussels

Office: Rue Montoyer 63, 6th floor
Tel: + 32-2-2831900
Fax: + 32-2-2831950
Email: edps@edps.europa.eu
Website: www.edps.europa.eu

From: [REDACTED]
Sent: 25 January 2012 15:28
To: HUSTINX Peter
Subject: RE: European-American Business Council: Meeting Request for 6-9 February

Dear Mr Hustinx,

Thank you for your reply. Based on your recommendations, we suggest a 1 hour meeting for Thursday, 9 February, from 17.00-18.00 CET. Please let me know if you are still available at this time. We have the address for your offices from the website and if you have other instructions, such as how far in advance of the meeting to arrive, please let me know.

Kind regards,

██████████
██████████
European-American Business Council
██████████

919 18th St, NW, Ste 220
Washington DC 20006

Work: +1 ██████████

Mobile: +1 ██████████
██████████

www.eabc.org

From: HUSTINX Peter [mailto:peter.hustinx@edps.europa.eu]
Sent: Tuesday, January 24, 2012 3:17 AM
To: ██████████
Cc: ██████████; ██████████; ██████████
Subject: RE: European-American Business Council: Meeting Request for 6-9 February

Dear Mr ██████████,

On the basis of your group's availability and my own current agenda, I would suggest a meeting (about one hour), either on Tuesday 7 February or on Thursday 9 February, both at the end of the afternoon (16.00-17.00 or 17.00-18.00).

Please let me know what suits you best.

Directions to the EDPS office are available at this link:
<http://www.edps.europa.eu/EDPSWEB/edps/cache/off/EDPS/Contact>

Kind regards,

Peter Hustinx

European Data Protection Supervisor (EDPS)
Contrôleur Européen de la Protection des Données (CEPD)
Mail: Rue Wiertz 60 - MO 63
B-1047 Brussels

Office: Rue Montoyer 63, 6th floor
Tel: + 32-2-2831900
Fax: + 32-2-2831950
Email: edps@edps.europa.eu
Website: www.edps.europa.eu

From: [REDACTED]
Sent: 20 January 2012 17:45
To: HUSTINX Peter
Cc: [REDACTED]; [REDACTED]; [REDACTED]
Subject: European-American Business Council: Meeting Request for 6-9 February

Dear Mr. Hustinx,

I'm writing to request an appointment with you for senior EABC member company executives and myself in the February 6-9 period. We'd like to discuss the EU Data Protection Framework and its implications for Trans-Atlantic and global commerce. [REDACTED], Oracle's [REDACTED] and EABC Data Governance Group US [REDACTED] suggested that we ask to see you on this issue.

The European-American Business Council is the largest Trans-Atlantic business association. We represent 70+ US, Canadian and EU-based global companies. Please find attached the EABC Membership, as well as the EABC Overview.

Our group's current availability on 6-9 February is:

- **6 February from 14:00-16:00 CET**
- **7 February from 10:30-18:00 CET**
- **8 February from 9:00-12:00 CET**
- **9 February from 15:00 – 18:00 CET**

Our group will include the following executives:

- [REDACTED], [REDACTED], Oracle
- [REDACTED], [REDACTED], Research in Motion
- [REDACTED], [REDACTED], Deutsche Post DHL
- [REDACTED], [REDACTED], European-American Business Council
- [REDACTED], [REDACTED], European-American Business Council

Thank you for your consideration of this request. Please let us know if you can see us that week.

Kind regards,



European-American Business Council

EABC [REDACTED] [REDACTED] WDC: [REDACTED] www.eabc.org

[Redacted]

From: [Redacted]
Sent: 08 February 2012 21:35
To: HUSTINX Peter
Cc: [Redacted]
Subject: European-American Business Council: Meeting Attendance for 6-9 February

Dear Mr. Hustinx,

Please find below the final attendance list from the EABC and our member companies for tomorrow's meeting, 9 February, from 17.00-18.00 CET. There has been great interest from our member companies in this meeting. Thank you in advance for taking the time to speak with us.

Please let me know if you have any questions. We have requested that all participants arrive 15 minutes early for security purposes. [Redacted] (Cc'd), EABC's [Redacted] [Redacted], will attend the meeting and is available to answer all logistical questions ([Redacted] mobile #: +[Redacted])

Participant	Company
[Redacted]	BT
[Redacted]	DP DHL
[Redacted]	IBM
[Redacted]	McKenna Long
[Redacted]	Microsoft
[Redacted]	Oracle
[Redacted]	RIM
[Redacted]	SAP
[Redacted]	EABC
[Redacted]	EABC

Kind regards,

[Redacted]
European-American Business Council
[Redacted]

919 18th St, NW, Ste 220

Washington DC 20006

Work: +1 [REDACTED]

Mobile: +1 [REDACTED]

[REDACTED]

www.eabc.org

From: HUSTINX Peter [mailto:peter.hustinx@edps.europa.eu]

Sent: Wednesday, January 25, 2012 9:38 AM

To: [REDACTED]

Subject: RE: European-American Business Council: Meeting Request for 6-9 February

Dear Mr [REDACTED],

OK for Thursday 9 February at 17.00-18.00 CET.

We will inform the guards at the reception of our European Parliament owned office building at Rue Montoyer 63. Registration of your delegation of six should not take more than 5 minutes.

Kind regards,

Peter Hustinx

European Data Protection Supervisor (EDPS)

Contrôleur Européen de la Protection des Données (CEPD)

Mail: Rue Wiertz 60 - MO 63

B-1047 Brussels

Office: Rue Montoyer 63, 6th floor

Tel: + 32-2-2831900

Fax: + 32-2-2831950

Email: edps@edps.europa.eu

Website: www.edps.europa.eu

[Redacted]

From: [Redacted]
Sent:
To: HUSTINX Peter
Subject: Request of meeting [Redacted] AT&T [Redacted]
[Redacted] 27-29 March

Dear Mr. Hustinx,
I hope this mail finds you well. I am contacting you to enquiry with you the possibility of setting up a meeting between you and Mr. [Redacted], [Redacted] at AT&T during the week of 27-29 March. [Redacted] will be in Brussels for the [Redacted] event on [Redacted] and would be grateful to have the opportunity of having an exchange of views with you on data privacy.

[Redacted] is responsible for [Redacted]
[Redacted] participates in [Redacted]
[Redacted]. In addition, he represents AT&T in [Redacted]
[Redacted]. He also has been actively engaged in [Redacted]

Would a meeting be of interest to you, [Redacted] could be available on 27 March in the morning, 28 and 29 of March at your best convenience.
I would be grateful if you could let me know whether you could be interest and available for a meeting and eventually indicate to me a day and timeslot that would be suitable to you.

Would you have any further questions, please don't hesitate to contact me

Kind Regards,
[Redacted]

[Redacted]
[Redacted]
[Redacted]
AT&T- 25, Rue d'Arlon – B-1050 Brussels
Tel: +32 [Redacted]
GSM:+32 [Redacted]
[Redacted]

[REDACTED]

From: [REDACTED]@humbrophy.com>
Sent:
To: HUSTINX Peter
Subject: Adobe Meeting Request

Dear Mr. Hustinx,

I'm writing to you on behalf of Adobe. On week starting 18 June, Mrs [REDACTED], [REDACTED] at Adobe Systems (based in San Jose, California) will be visiting Brussels. Could you possibly find a moment in your calendar while she is here to share thoughts on a number of matters arising from the **new data protection rules**?

While Adobe is, historically, best known for creating PDF, these days their business is focused around helping organizations create, manage and monetize their content. We're one of the large providers of web analytics technologies – the software that makes websites work effectively - in the world.

I look forward to hearing your availabilities.

Thanks in advance for your time and consideration.

Best regards,

[REDACTED]
[REDACTED]

41 Rue de la Science, 1040 Brussels, Belgium

T: +32 [REDACTED]
M: +32 [REDACTED]
M: +32 [REDACTED]

E: [REDACTED] [\[REDACTED\]@humbrophy.com](mailto:[REDACTED]@humbrophy.com)

32 Merrion Street, Dublin 2, Ireland T: +353 (0) 1 662 4712 F: +353 (0) 1 662 4714
One Fetter Lane, London, EC4A 1JB, UK T: +44 (0) 20 3440 5656 F: +44 (0) 20 3440 5664

www.humbrophy.com

This e-mail is from HUME BROPHY. The e-mail and any files transmitted with it are confidential and may also be privileged and intended solely for the use of the individual or entity to whom they are addressed. Any unauthorised direct or indirect dissemination, distribution or copying of this message and any attachments is strictly prohibited.

[REDACTED]

From: HUSTINX Peter
Sent: 05 June 2012 13:50
To: [REDACTED]
Subject: RE: Request for a meeting

So meeting on June 26 at 11.00-11.45 now confirmed.

From: [REDACTED]@SIIA.net]
Sent: 05 June 2012 13:42
To: HUSTINX Peter
Subject: Re: Request for a meeting

Mr. Hustinx,

Thank you very much. I look forward to seeing you on June 26 at your office at Rue Montoyer.

Best,

[REDACTED]
[REDACTED]
[REDACTED]
Software & Information Industry Association
[REDACTED]

From: HUSTINX Peter [mailto:peter.hustinx@edps.europa.eu]
Sent: Tuesday, June 05, 2012 06:14 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Request for a meeting

Dear Mr [REDACTED],

I would be available for a meeting on June 26 - preferably at 11.00-11.45 - in my office at Rue Montoyer
<http://www.edps.europa.eu/EDPSWEB/edps/cache/off/EDPS/Contact>.

Alternatively, perhaps in the course of the afternoon - in that case, please check with my secretary (in copy).

Please note that I will not be available on June 27, due to commitments elsewhere.

Kind regards,

Peter Hustinx

European Data Protection Supervisor (EDPS)
Contrôleur Européen de la Protection des Données (CEPD)
Mail: Rue Wiertz 60 - MO 63
B-1047 Brussels

Office: Rue Montoyer 63, 6th floor
Tel: + 32-2-2831900
Fax: + 32-2-2831950
Email: edps@edps.europa.eu

From: [REDACTED] SIIA.net]
Sent: 04 June 2012 20:23
To: HUSTINX Peter
Subject: Request for a meeting

Mr. Hustinx,

I am writing to request a meeting with you on the issues raised by the EU's draft data protection regulation. I will be in Brussels on June 26 and June 27 and could meet at a convenient time during those days.

I run the [REDACTED] in the Software & Information Industry Association. You can find out more about us at www.sii.net. Our major members include a number of worldwide and European companies including IBM, Oracle, Adobe, Google, Reed Elsevier, Pearson, News Corp, Google, Intuit, Red Hat and McAfee. A number of my member companies mentioned to me that you would be a good person to speak to on these issues. I would seek to discuss the major issues our members see in the proposal and tentatively provide some specific ways forward to resolve them.

I would be grateful if we could find a time to meet.

Best,

[REDACTED]

[REDACTED]

[REDACTED]

Software & Information Industry Association

[REDACTED]

Washington, DC 20005

[REDACTED]

[Redacted]

From: [Redacted] amchameu.eu>
Sent:
To: European Data Protection Supervisor
Subject: AmCham EU request for a meeting to discuss data protection



Dear Mr. Hustinx,

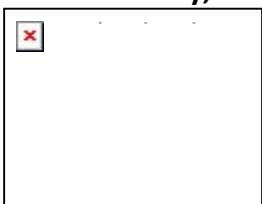
I'm contacting you on behalf of the American Chamber of Commerce to the EU's (AmCham EU) Digital Economy Committee.

Our Committee is currently finalising a position paper on data protection which you will receive soon and we have and continue to follow closely the discussions both in the EU and the US on data protection. We would be grateful for the opportunity to discuss this important issue with you and to highlight some of our priorities on data protection in the coming weeks.

We are particularly eager to learn from you how you see the discussion around data protection progress in the context of the ongoing developments in the EU Institutions.

We would like to propose a meeting during the weeks of July 9th, 16th and 23rd. Please do not hesitate to contact me on + [Redacted] if you would like any further details.

Yours sincerely,



[Redacted]
[Redacted] AmCham EU

[REDACTED]

From: [REDACTED]@humbrophy.com>
Sent: 05 July 2012 11:32
To: European Data Protection Supervisor
Cc: [REDACTED]@humbrophy.com
Subject: Meeting request [REDACTED], [REDACTED] for Adobe Systems, Washington D.C.

Dear [REDACTED],

Many thanks for taking my call this morning and for assisting in organising the meeting.

I wish to confirm the meeting between Mr [REDACTED], [REDACTED] for Adobe Systems Incorporated and Mr Peter Hustinx on Friday 20 July 2012 at 2pm at the EDPS office on Rue Montoyer 63.

I will advise Mr [REDACTED] to meet you at reception as suggested.

Many thanks again for your help,

Kind regards,

[REDACTED]

From: [REDACTED]@humbrophy.com]
Sent:
To: 'peter.hustinx@edps.europa.eu'
Cc: [REDACTED]
Subject: Meeting request [REDACTED], [REDACTED] for Adobe Systems, Washington D.C.

Dear Mr Hustinx,
I'm writing to you on behalf of Adobe Systems.
Mr [REDACTED], [REDACTED] for Adobe Systems Incorporated, would welcome an opportunity to discuss the new Data Protection Regulation with you.
[REDACTED] who is based in Adobe's Washington D.C. office, will be in Brussels from 19-20 July 2012.
In Washington, Mr [REDACTED] works with [REDACTED] and [REDACTED] on a range of [REDACTED] issues. He previously served with the [REDACTED] in the [REDACTED] and on the staff of [REDACTED] before coming to Adobe in [REDACTED].
Any meeting opportunities you have in your calendar for the dates, 19 – 20 July (excluding the morning of 20 July), would be very welcomed.
Should you require any additional information, please do not hesitate to contact me.
Looking forward to hearing from you,
Kind regards,

--

[REDACTED]
[REDACTED]

41 Rue de la Science, 1040 Brussels
T: +32 [REDACTED]
F: +32 [REDACTED]
M: +32 [REDACTED]
E: [REDACTED]@humbrophy.com

We have recently opened our Paris office

32 Merrion Street Upper, Dublin 2, Ireland T: +353 (0) 1 662 4712
21 Boulevard Haussmann, 75009 Paris, France T: +33 (0) 1 5603 6589
One Fetter Lane, London, EC4A 1BR, UK T: +44 (0) 20 3440 5656



www.humbrophy.com

This e-mail is from HUME BROPHY. The e-mail and any files transmitted with it are confidential and may also be privileged and intended solely for the use of the individual or entity to whom they are addressed. Any unauthorised direct or indirect dissemination, distribution or copying of this message and any attachments is strictly prohibited.

[REDACTED]

From: [REDACTED]
Sent: 13 July 2012 10:21
To: HUSTINX Peter
Subject: AmCham EU – Position paper on the General Data Protection Regulation
Attachments: AmCham EU - Position Paper on Data Protection 20120711.pdf



Dear Mr. Peter Hustinx,

The American Chamber of Commerce to the European Union (AmCham EU) and in particular its Digital Economy Committee [REDACTED] would like to present you with its position on the *General Data Protection Regulation*. The paper incorporates and builds upon our responses to previous Commission consultations on the European Union's approach to the protection of personal information.

We welcome the opportunity to express our position on the *General Data Protection Regulation* and we hope our comments will assist the European Institutions in adopting a sound text for the development of an efficient EU Data Privacy legislation, allowing protection of the EU citizens privacy and at the same time market players to invest in the infrastructures and services which will benefit both citizens and business.

I hope you will find this paper useful and I am looking forward to discuss this paper with you in the upcoming weeks. If you have any questions or comments on this paper please do not hesitate to contact me [REDACTED] or [REDACTED] [REDACTED] or tel: +32 [REDACTED]).

Yours sincerely,



[Redacted], AT&T
[Redacted], AmCham EU

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate U.S. investment in Europe totaled \$2.2 trillion in 2010 and directly supports more than 4.2 million jobs in Europe.

AmCham EU | Avenue des Arts/Kunstlaan 53 | B-1000 | Brussels | Tel. +32 [Redacted] | info@amchameu.eu | www.amchameu.eu

[Redacted]

From: [Redacted] symantec.com>
Sent:
To: HUSTINX Peter; BUTTARELLI Giovanni
Cc: [Redacted]
Subject: Meeting request

Dear Mr. Hustinx, Mr. Buttarelli,

I hope you are doing well. May I take the opportunity to warmly wish you personal and professional success in 2013. I am writing you because I was wondering if it would be possible to arrange a short meeting in Brussels sometime before mid February.

The purpose of the meeting would be to discuss about the review of the data protection framework and in particular about some of the points around information security and the right to be forgotten. I would like to share some of our ideas with you which I believe promote the objectives of the Regulation to protect individual privacy.

I will be looking forward to hear from you. Sincerely yours

[Redacted]

[Redacted]

[Redacted]

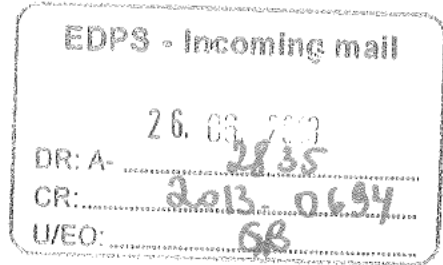
www.symantec.com

Office: [Redacted]
Interoffice: [Redacted]
Mobile: [Redacted]
Fax: [Redacted]
Email: [Redacted] [symantec.com](mailto:[Redacted]@symantec.com)



This message (including any attachments) is intended only for the use of the individual or entity to which it is addressed and may contain information that is non-public, proprietary, privileged, confidential, and exempt from disclosure under applicable law or may constitute as attorney work product. If you are not the intended recipient, you are hereby notified that any use, dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, notify us immediately by telephone and (i) destroy this message if a facsimile or (ii) delete this message immediately if this is an electronic communication.

From: [REDACTED]
Sent: 25 June 2013 20:32
To: BUTTARELLI Giovanni
Cc: [REDACTED]
Subject: RE: Requesting Meeting with Giovanni Buttarelli



Dear Mr. Buttarelli,
 I agree that maybe it is best to wait to schedule a time with [REDACTED] until there is a confirmation on your other commitment. I will follow-up with you on Monday if I have not heard from you concerning the Council's decision.

Please let me know if you will be attending the USEU 4th of July celebration. If so, perhaps there is a chance for you and [REDACTED] to meet at that time.

[REDACTED] will be interested in speaking with you about the "right to be forgotten" figuring prominently in the new EU draft data protection legislation. As well, he will be interested in learning your thoughts on how the U.S. and the EU can build an interoperable data privacy regime to facilitate trade.

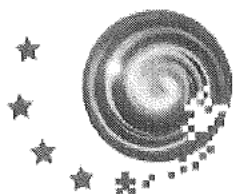
If there are any additional topics you would like to discuss with [REDACTED] please let me know.

Best regards,
 [REDACTED]

This email is UNCLASSIFIED.

From: BUTTARELLI Giovanni [mailto:giovanni.buttarelli@edps.europa.eu]
Sent: Tuesday, June 25, 2013 9:26 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Requesting Meeting with Giovanni Buttarelli

Dear Mr. [REDACTED]
 thank you for your message.
 We're still waiting for a confirmation from the Council of the EU about the scheduled afternoon session of that day on our 2014 budget.
 It is supposed to be in between 14,30 and 17,00, for around one hour and half as a maximum.
 What I suggest at this stage, unless we may re-schedule our meeting in the second part of the morning before 14,30, is to keep in touch and wait for the Council's confirmation and check our calendars accordingly.
 Best regards
 Giovanni Buttarelli




Giovanni Buttarelli
Assistant Supervisor

Tel. +32 2 283 19 02 | Fax +32 2 283 19 50

giovanni.buttarelli@edps.europa.eu

European Data Protection Supervisor
 Postal address: Rue Wiertz 60, B-1047 Brussels
 Office address: Rue Montoyer 30, B-1000 Brussels

 @EU_EDPS www.edps.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

From: [REDACTED]
Sent: 21 June 2013 22:33
To: BUTTARELLI Giovanni
Cc: [REDACTED]
Subject: RE: Requesting Meeting with Giovanni Buttarelli

Dear Mr. Buttarelli,
 U.S. Coordinator [REDACTED] requests re-scheduling his meeting with you to 16.00 on Thursday, 4 July. Please advise as to your availability.

I will also endeavor to provide you a list of topics we plan to discuss once we confirm the new appointment time.

Kind regards,

[REDACTED]
U.S. Department of State

[REDACTED]
Washington, D.C.

Office: +1 [REDACTED]

Email: [REDACTED]@state.gov

This email is UNCLASSIFIED.

From: [REDACTED]
Sent: Monday, June 17, 2013 5:14 PM
To: 'BUTTARELLI Giovanni'
Cc: [REDACTED]
Subject: RE: Requesting Meeting with Giovanni Buttarelli

Dear Mr. Buttarelli,
 Thank you for confirming your availability to meet on Thursday, 4 July at 11 a.m. I will provide you a list of suggested topics later this week.

Attending for the U.S. delegation will be [REDACTED] and [REDACTED] along with senior advisors [REDACTED] [REDACTED] and me.

Best regards,

[REDACTED]
U.S. Department of State

[REDACTED]
Washington, D.C.

Office: + [REDACTED]

Email: [REDACTED]@state.gov

This email is UNCLASSIFIED.

From: BUTTARELLI Giovanni [mailto:giovanni.buttarelli@edps.europa.eu]

Sent: Sunday, June 16, 2013 3:32 PM

To: [REDACTED]

Cc: giovanni.buttarelli@edps.europa.eu; [REDACTED]

Subject: Re: Requesting Meeting with Giovanni Buttarelli

Dear Mr. [REDACTED],

thank you for your message.

I am available for an exchange of views and I have blocked one hour for Thursday the 4th, at 11:00, being outside Brussels the day after.

Please be free, where appropriate, to share in advance the topics they prefer to touch in the meeting.

Our office is Rue Montoyer, 30, 6' floor. Their ID can be simply showed at he main entrance.

Ms. [REDACTED] from my Secretariat remains at your disposal for any further need in terms of logistics.

Best regards

Giovanni Buttarelli

Il giorno 14 Jun 2013, alle ore 16:13, "[REDACTED]" ha scritto:

Dear Mr. Buttarelli,

[REDACTED], [REDACTED], and [REDACTED]

[REDACTED] will be traveling to Brussels on 4 and 5 July. They would like to meet with you, preferably anytime after 10:30 a.m. Thursday, 4 July or after 2:30 p.m. Friday, 5 July.

Mr. [REDACTED] met Peter Hustinx recently in Washington, D.C. and very much appreciated the exchange of views on data protection. He is very interested in meeting with you as well to continue the discussion.

Please let me know if you would be available to meet and the time that would be most convenient for you.

Kind regards,

[REDACTED]
U.S. Department of State

[REDACTED]

Washington, D.C.

Office: + [REDACTED]

Email: [REDACTED]@state.gov

This email is UNCLASSIFIED.

[REDACTED]

From: [REDACTED]
Sent: [REDACTED]
To: [REDACTED]
Subject: RE: Meeting request: Hewlett-Packard (21 or 22 January)

Dear Mr [REDACTED],

On behalf of Mr Buttarelli, I inform you that he will very pleased to meet Mr [REDACTED] in our premises on 22 January at 11 am.




Could you please confirm me it is still available and if he will be accompanied as I need to ask the permissions to the building?

Many thanks in advance.

Kind regards,



[REDACTED]
Administrative assistant

 |  (+32) [REDACTED]
 [REDACTED]

European Data Protection Supervisor

Postal address: Rue Wiertz 60, B-1047 Brussels

Office address: Rue Montoyer 30, B-1000 Brussels

 @EU_EDPS  www.edps.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

From: [REDACTED]@communitygroup.eu]
Sent: 08 January 2015 15:39
To: BUTTARELLI Giovanni; wojtek.wiewiorowski@edps.europa.eu
Subject: Meeting request: Hewlett-Packard (21 or 22 January)

Dear Mr. Buttarelli
Dear Mr. Wiewiórowski,

Let me first of all congratulate you on your recent appointment at the head of the European Data Protection Supervisor and wish you all the very best in your new functions.

It is my pleasure to write to you today on behalf of Mr. [REDACTED] [REDACTED] [REDACTED] at Hewlett-Packard (HP). Mr. [REDACTED] will be in Brussels on the occasion of the Computers, Privacy

and Data Protection (CPDP) Conference and would like to request a meeting with you **on 21 January in the afternoon or on 22 January at 11am or in the afternoon.**

As the [REDACTED] of HP's [REDACTED] team, Mr. [REDACTED] would be happy to have the opportunity to meet with you to discuss his latest views on the General Data Protection Regulation and to provide HP's view on the issue of accountability, BCRs and the one-stop-shop mechanism. Furthermore, as cross-border data flows are a key component of HP's business, Mr. [REDACTED] would also be happy to discuss the issue of Safe Harbor and elaborate on how HP supports the constructive conclusion between the EU and US on the agreement.

Please do not hesitate to contact me with any queries on this matter.

Many thanks in advance for your kind consideration.

[REDACTED]

[REDACTED]

Community Public Affairs

6 Place Poelaert - 1000 Bruxelles - Belgium

Mob: +32 [REDACTED]

Tel: +32 [REDACTED]

Fax: +32 [REDACTED]

Mail to: [REDACTED] [communitygroup.eu](mailto:[REDACTED]@communitygroup.eu)

Learn more: www.communitypublicaffairs.eu

This email is confidential and may be subject to legal or other professional privilege. It is also subject to copyright. If you have received it in error, confidentiality and privilege are not waived and you must not disclose or use the information in it. Please notify the sender by return email and delete it from your system.

Edelman is the world's largest public relations firm, in 13 markets across Europe & CIS, and over 65 offices and more than 5,000 employees worldwide, as well as affiliates in more than 35 cities.

Benelux Agency of the Year (Holmes Report 2014)
Best Pan-European Agency to Work For (Sabre Awards 2013)
European Agency of the Year (European Excellence Awards 2013)
International Consultancy of the Year (PRCA Awards 2013)
Global Agency of the Year (Global Sabre Awards 2013)

From: [REDACTED]
Sent: 09 January 2015 13:38
To: [REDACTED]
Subject: RE: Meeting Request: [REDACTED], [REDACTED] and [REDACTED], [REDACTED], General Electric - Brussels

Dear [REDACTED],

Our address is **Rue Montoyer 30**. When they arrive to the reception, please tell them to ask for me so I can accompany them to Mr Buttarelli's office.

Have a nice weekend.

Kind regards,

[REDACTED]

From: [REDACTED]@edelman.com]
Sent: 09 January 2015 12:50
To: [REDACTED]
Subject: RE: Meeting Request: [REDACTED], [REDACTED] and [REDACTED], [REDACTED], General Electric - Brussels

Dear Mrs [REDACTED],

Many thanks for your reply. I hereby confirm Mr [REDACTED] and [REDACTED] availability to meet Mr Buttarelli on Monday 2 February at 15.00pm.

Kindest regards,

[REDACTED]

From: [REDACTED]
Sent: 09 January 2015 12:01
To: [REDACTED]
Subject: RE: Meeting Request: [REDACTED], [REDACTED] and [REDACTED], [REDACTED], General Electric - Brussels

Dear Madam,

On behalf of Mr Giovanni Buttarelli, I will inform you that he will very pleased to meet both Mr [REDACTED] and Mr [REDACTED] on the date you proposed so 2 February in the afternoon as of 15.00 if it is suitable for you, of course.

I will wait for your confirmation and I will send you the address.

Kind regards,



[REDACTED]
Administrative assistant

[REDACTED] | (+32) [REDACTED]

[REDACTED]

European Data Protection Supervisor

Postal address: Rue Wiertz 60, B-1047 Brussels

Office address: Rue Montoyer 30, B-1000 Brussels

@EU_EDPS www.edps.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

From: [REDACTED]@edelman.com]

Sent: 05 January 2015 14:26

To: European Data Protection Supervisor

Subject: Meeting Request: [REDACTED], [REDACTED] and [REDACTED], [REDACTED], General Electric - Brussels

Dear Mr Buttarelli,

On behalf of [REDACTED], [REDACTED] and [REDACTED], [REDACTED] at General Electric (GE) we would like to enquire whether you would be available for a meeting, anytime at your convenience, on the week of February 2nd, in Brussels.

This meeting will be an opportunity to introduce GE, and to exchange views on the current state of play of the negotiations on the EU reforms of data protection, ahead of the next EU justice and home affairs meetings.

Mr. [REDACTED] has been the [REDACTED] of General Electric since [REDACTED]. In this role, he oversees the [REDACTED] of GE's [REDACTED]. He also works closely with GE's Government Affairs team on [REDACTED], as well as the [REDACTED].

Given your involvement in the discussion of these issues we would most appreciate an opportunity to meet with you.

We look forward to your response. Please allow us to take the liberty of contacting your office shortly to see if there is a convenient time to arrange this meeting.

Kindest Regards,

[REDACTED]

[REDACTED]

Edelman Brussels

28 Av. Marnixlaan, B-1000 Brussels, Belgium

t: +32 [REDACTED] m: +32 [REDACTED] | ext: [REDACTED]

w: www.edelman.com

Edelman is the world's largest public relations firm, in 13 markets across Europe & CIS, and over 65 offices and more than 5,000 employees worldwide, as well as affiliates in more than 35 cities.

Benelux Agency of the Year (Holmes Report 2014)

Best Pan-European Agency to Work For (Sabre Awards 2013)

European Agency of the Year (European Excellence Awards 2013)

International Consultancy of the Year (PRCA Awards 2013)

Global Agency of the Year (Global Sabre Awards 2013)



Edelman kindly reminds you to think before you ink.

Innovative use of data in an industrial context:

The Need for a Balanced Approach to the Draft General Data Protection Regulation

In “Pushing the Boundaries of Minds and Machines”, GE explains why the “Industrial Internet” holds the potential of significantly transforming the economy and of bringing substantial economic benefits in terms of faster economic growth and higher living standards. According to estimates, the Industrial Internet could add EUR 2 trillion to Europe’s GDP by 2030, by achieving efficiency gains as a result of connected machines and real time data analytics.¹

This paper discusses the role that personal data plays in the Industrial Internet. In particular, it explains the need – particularly in light of ongoing discussions concerning the draft General Data Protection Regulation -- to consider both the *context* in which personal data is used, and to design proportional responses to the associated *risk* when regulating the use and transfer of such data.

The role of personal data in the Industrial Internet

The Industrial Internet is a growing economic reality that consists in connecting machines-to-machines, and machines-to-people-to-machines, to improve safety, efficiency and the performance of machines. For this purpose, the collection of personal data is limited when compared to the personal data collected in the context of the Consumer Internet. The core function of the Industrial Internet is **not** to collect vast amounts of personal data to create individual profiles for marketing or data brokerage. Rather, at the heart of the Industrial Interest are the vast quantities of data generated by machines, and the advanced algorithms that convert these data into actionable information for use by equipment operators. By remotely aggregating these data and applying unique software-based algorithms, equipment anomalies can be rapidly identified and repaired, and safety, unit performance, efficiency and reliability can be enhanced. In some cases, this may include the collection of personal data for the purpose of a functional machine-to-machine communication or to correct errors in machines that affect the home, transportation, energy, or the provision of healthcare services. For example, limited information about mechanic services or passenger weight may be needed for flight diagnostics, and information concerning patient weight or age may be needed to support proper healthcare diagnostic results and equipment support.

Examples from the transportation, energy and healthcare sectors help to illustrate the use of machine data in an Industrial Internet setting.

In both **transportation** and **energy**, data generated by machines, such as aircraft or locomotive engines, and turbines for power generation, can be used to improve infrastructure efficiency and safety over time. The data concerning machine performance is communicated over the internet to computing facilities, where it is analysed in real-time. A single turbine can generate up to 50 gigabytes of data per day, while an aircraft or locomotive engine can generate thousands of pieces

¹ *Industrial Internet: A European Perspective. Pushing the Boundaries of Minds and Machines*, June 2013
http://www.ge.com/europe/downloads/IndustrialInternet_AEuropeanPerspective.pdf

of data instantaneously concerning fuel flow, engine temperature and the effect of environmental conditions. In both of these scenarios, a limited amount of personal information concerning machine operation may be analysed, and it is likely – particularly in transportation – that data will cross national borders along with the underlying equipment. Using these data in an Industrial Internet setting generates important efficiency savings. For instance, an efficiency increase of only 1% in gas-fired power generation installed base alone represents EUR 11 billion in fuel savings in Europe over the next 15 years. The same holds true in aviation. The European commercial airline sector spends about EUR 35 billion per year on jet fuel. Industrial Internet efficiency savings of 1% would represent nearly EUR 6.5 billion in fuel cost savings over 15 years.

The **healthcare** sector also stands to gain in efficiency and cost reduction through the innovative use of data. Analysing healthcare data allows hospitals and other providers to move from episodic care to a more integrated patient-centric approach in healthcare delivery. At the same time, analytics empower research and innovation in Europe to drive better health outcomes, increase productivity and contribute to economic growth. Over EUR 1.2 trillion was spent on healthcare in the EU in 2012. It is estimated that 10% of this expenditure is wasted due to system inefficiency, of which 59% is in clinical and operations inefficiency. This is where the Industrial Internet could yield the greatest benefits: a 1% efficiency increase in these clinical and operations would translate into EUR 11 billion of savings over the next 15 years. These are important savings in light of Europe's ageing population particularly given that public healthcare budgets are under severe pressure.

A patient's hospital stay – even for relatively straightforward care – involves hundreds of people, processes and assets. The medical outcome and cost of that care, as well as the quality of the patient's experience, depend on how efficiently and effectively all of these resources are integrated and managed. The effective use of data optimises the operations of hospitals by improving asset management and optimising patient flows.

The infograph below provides an example where available data is used real-time to improve operations that can have a significant impact on Hospital Acquired Infections (HAI), thereby reducing the number of infections with patients. HAIs are an unintended consequence of care delivered by healthcare organisations. As shown here, a hospital may use a variety of data, including sensor readings when a care provider enters a room, to determine whether care protocols – in this case related to hand washing - are being followed, as well as to research whether care protocols or hospital design should be modified to improve overall care in a hospital or across one or more medical systems. Though the data is initially used to manage current healthcare operations, some data may be needed to perform longer-term research into equipment fixes and improvements and into care protocols.

THE HUMAN SIDE OF DATA

People go to hospitals to get well. Unfortunately, many will become even sicker because of exposure to bacteria and other germs. They will be the unwilling recipients of **Hospital-Acquired Infections**, known as HAIs.

1 IN 20 PATIENTS WILL GET AN HAI 99,000 WILL DIE

Previous methods to track handwashing proved inaccurate, costly and inefficient.

HOWEVER, EMPOWERING PEOPLE WITH INFORMATION AND TOOLS MAKES A BIG DIFFERENCE.

AGILETRAC
is core to the handwashing monitoring system that closes the gap between intuition and reality. Information-sharing and alerts lead to healthier outcomes.

1. SENSORS
2. COMPLIANCE TRACKING
3. REAL-TIME MEASUREMENT

WITH AWARENESS COMES ACTION

When people feel informed about their behavior they are more likely to react and change it.

REAL-TIME RESULTS **FEEDBACK** **TRANSPARENCY**

A 30% sustained improvement was realized in the first eight weeks after implementing AgileTrac.
The automated system collects better data quality and highly detailed samples.

THE RESULTS

HANDWASHES TRACKED / YR.

THEN	NOW
700 <small>OBSERVED</small>	1.8M <small>AUTOMATED</small>

Safer handwashing procedures have the potential to:
reduce the number of HAIs
decrease risk to patients and caregivers

DATA BECOMES A POWERFUL TOOL FOR COLLABORATION.

HCA
Hennepin County
SUMMERVILLE
SOLUTIONS

SOURCE:
New York: Center for Health Care Associated Infections and Deaths in U.S. Hospitals, 2002. Centers for Disease Control and Prevention, Public Health Report (November 2007) Atlanta, GA.
AgileTrac Results, © HCA Summerville Case Study, 2012.

A hand washing monitoring system uses real-time data via sensors to improve compliance of hygiene protocols. The results: a 30% sustained improvement was realised in the first eight weeks after implementing the monitoring system, and an 80% increase of care protocol compliance: from 700 observed hand washes to 1.8 million tracked hand washes on an annual basis, thereby significantly reducing the number of infections of patients with Hospital Acquired Infections.

The Need to Consider *Context* and *Proportional Responses to Risk* when Regulating Data

Throughout the drafting process, the General Data Protection Regulation has been promoted as a means to lower barriers to innovation and to productive uses of data and promoting a risk-based approach to data protection governance. As EU Justice Commissioner Reding explained when issuing the first draft, the GDPR is intended to *“help build trust in online services . . . while making life easier and less costly for businesses. A strong, clear and uniform legal framework at EU level will help to unleash the potential of the Digital Single Market and foster economic growth, innovation and job creation.”*

The hand washing case described above is just one example of the innovative use of data in a healthcare setting that can provide opportunities for growth of innovative technologies across Europe while also improving patient care and hospital efficiency. It is, however, also an example where important and innovative uses of data will only be fostered by a regulatory environment that focuses on the ways in which data will be used and on how organizations address risks of loss or misuse rather than creating more administrative burdens and undue limitations on its use.

While a streamlined regulatory environment holds out the prospect of such benefits to industry and to consumers, the current discussions of the GDPR give rise to concern. Some of the most notable issues with the current drafts under consideration are discussed below.

Consent: Article 6 (Lawfulness of Processing) and Article 7 (Conditions for Consent) of the LIBE draft require that individuals be notified of, and give “explicit consent” to, each specific purpose for which data is processed, and consent would lose its validity once the initial purpose given for the collection of data is no longer necessary. Moreover, Article 7 of the LIBE draft provides that Member States may enact further specifications in these areas, including purpose specification, processing and storage. These proposals contrast with existing data protection law, and with the Council’s current proposal, which provide for “unambiguous consent” and protects uses that are compatible with the initial purpose of collection.

These requirements, as well as the prospect of further limitations from each Member State, would be particularly difficult for organisations whose products are used in a complex supply chain, since it would be difficult to ascertain whether proper consent exists to use data for important purposes such as equipment support and avoiding “regression” of problems as new versions of healthcare solutions and other products are released. It would be difficult, at best, for individuals to consent to all potential legitimate uses of data for machine analytics and long-term care given the complexity of the relationships involved with infrastructure, transportation and healthcare systems. However, without such consent, organisations may not be able to use data to address safety and efficiency issues in products or in people’s interaction with those products. Thus, in the example above, consent for collection and use of patient data for care may be deemed insufficient to read and analyse hand washing data either for care or for measuring improvement in clinical outcomes.

Privacy Impact Assessments: An important goal of the GDPR was to remove the varying and sometimes inconsistent registration requirements across the Member States, which are burdensome and generally have not proven to materially improve protection of data. However, under the current

drafts, organizations would be required to perform detailed privacy impact assessments and make those assessments available for review by individual Member State DPAs in light of different factors, including in cases where the processing involved new technology. Thus, the most innovative uses of technology may be subject to the highest level of scrutiny. Moreover, since the requirement to perform a privacy impact assessment (“PIA”) extends to a range of undefined circumstances beyond those already defined in the law (such as where processing would involve “sensitive data”), there is significant risk that the PIA requirement would be interpreted differently by the Member States, leading to both greater administrative burden and splintered or conflicting regulation of new technologies that otherwise would serve a single market across the EU. In order to avoid the PIA requirement becoming a complex administrative burden and a significant disincentive to innovation, the obligation to perform PIAs should be limited to circumstances involving sensitive data, as defined, and controllers should be provided explicit protection against the disclosure of PIAs that could reveal trade secret information and other intellectual property.

Cross Border Data Flows: In recent months there has been a significant amount of discussion in the context of the Regulation about a perceived need to restrict cross-border transfers in order to better protect the privacy of EU citizens. By way of example, Article 43a of the LIBE draft, which would require DPA approval before records could be disclosed to law enforcement and others outside the EU, would create direct conflicts of law for many organizations operating -- including those headquartered – in the EU. Some involved in the negotiations have suggested going farther in limiting cross-border data flows.

Industrial Internet services are by definition without boundaries, and cross border data flows should be allowed as long as the data is bound to be protected in a manner consistent with EU data protection standards. A focus on managing risk would permit significantly greater innovative use and transfer of data without adding materially to the associated risk. From the perspective of the Industrial Internet, cross border data flows should remain lawful while maintaining adequate protection of personal data.

Damages: The LIBE draft includes the potential for damages up to 5% of a company’s global turnover, and some involved in the negotiations have called for that number to be revised up to 10% (in the case of GE, this could theoretically amount to as high as \$15 billion for a single data protection incident). There currently is no provision limiting damages in light of the organization’s overall data protection program, the nature of the harm suffered or the intent of the organization. The current proposed framework, and particularly the uncertainty concerning regulatory enforcement for a single incident, would provide a significant disincentive to organizations hoping to conduct business involving innovative technologies in the EU. By clarifying the damages available for incidents, as well as mitigating factors designed to encourage good data practices, the GDPR would promote strong data protection practices rather than discouraging investment in local innovation.

Conclusion

The use of Big Data for the Industrial Internet can provide significant economic and social benefits. However, regulating the use of data for industrial purposes purely in terms of narrowly granted one-to-one consent and permissions for point-to-point transfers would dramatically impede the value and benefit of Big Data in the industrial context, without providing significantly greater protections

for individuals. Similarly, re-asserting burdensome administrative requirements and imposing open-ended damages for privacy harms would create significant disincentives to investment in new technologies in the EU.

Instead, in the context of industrial use of machine data, it would be both more efficient and ultimately more protective to focus on *context* (how data is used and whether the use is reasonably anticipated) and *risk* (protecting data appropriately through security, monitoring and de-identification where possible). This would permit data to be used to improve and ensure the safety of machines, while also requiring that data be kept securely and not be used for unanticipated purposes.

[REDACTED]

From: [REDACTED]
Sent:
To: European Data Protection Supervisor
Cc: [REDACTED]
Subject: GE -- thank you
Attachments: GDPR-GE.final.pdf; FPF de-id_1 31 15..pdf

Dear. Giovanni,

My sincere, if belated, thanks for meeting with [REDACTED] and me at your office to discuss the draft GDPR. It was a wonderful discussion, and we appreciated your insights into your new role, as well as your forward-looking approach to privacy and innovation in Europe.

Please find attached the two papers we discussed, one a GE paper discussing the GDPR as it relates to GE's businesses in Europe, the other a draft paper from the Future of Privacy Forum proposing a path forward on technical and administrative de-identification to facilitate product research without risking data misuse. Please feel free to share these with colleagues if helpful. As suggested, we are working with Future of Privacy Forum to develop use cases that we can share as well.

Please let us know if we can be of assistance as you consider these issues. And we both look forward to seeing you today in Washington and to hearing your presentation tomorrow.

Best regards,

[REDACTED]

[REDACTED]

GE Corporate Legal

T [REDACTED]
F [REDACTED]

3135 Easton Turnpike
Fairfield, CT 06828 USA
General Electric Company

[GE imagination at work](#)



De-identification White Paper DRAFT Jan. 31, 2015

By Jules Polonetsky, Christopher Wolf, and Kelsey Finch

The current de-identification landscape is rife with uncertainty and risk for organizations, consumers, and regulators alike. While the policy debate continues to assume a binary framework where personal information is either identified or not, already a wide range of intermediary approaches appear in practice. Predicated on disagreements and misunderstanding about what data is or should be considered de-identified, the divide between how de-identification techniques are discussed and how they are deployed continues to grow. In order to find a path forward, we must change both how de-identification is discussed and how it fits within broader data protection and privacy debates.

This paper seeks to describe the current de-identification debate and explain the basis for the discord among policymakers and stakeholders. Next, we reframe the data spectrum, placing personal information that has been subjected to technical and/or administrative controls into three categories with different sets of controls and privacy protections applying to each set. Then, we examine the relevance of our approach to the existing U.S. and EU frameworks, both in theory and in practice. Finally, we describe critical measures for the success of de-identification and pseudonymization, so that important data uses can advance in a manner that considers both their benefits and risks.

Introduction

Since long before the computer age, consumers' personal information has been used to drive new product development and help organizations maintain their current services. Even in the pre-industrial age shopkeepers recorded their customers' transactions and purchasing habits, census takers collected individual demographic information by hand, and communities allocated resources on the basis of personal information. Modern computational power has magnified these activities, unleashing the era of Big Data where sophisticated analytics and large, detailed databases work together constantly to put personal data to new uses. Today, personal data are driving scientific and medical advances, more inclusive curricula, more efficient infrastructure, and a revolutionary wave of innovative technologies and services around the globe. In numerous fields of inquiry, researchers are putting geolocation, health, traffic, education, environmental, census and mobile carrier data, among others, to new and unanticipated uses. Even when collected to provide or maintain services, personal data can support secondary analysis on a vast scale. The ability to track and analyze various data trends over time has led to advances in education, health, public services, business and technology to the benefit of both individuals and society. Appendix A to this document provides a number of detailed examples of such uses of data.¹

¹ Appendix A forthcoming.

In today's world, researchers believe that additional advances will be achievable if they have access to increasingly extensive and detailed sets of information. Researchers depend on personal and quasi-personal data to improve equipment and analytics engines across every industry. Their impact can already be seen in new tools and techniques helping to make x-ray machines better, drugs safer and more effective, and transportation more secure. Much of this societally beneficial research also takes place in private hands. In the business world, just as in scientific communities, access to larger and more detailed data sets is seen as a door to better and safer products, more helpful customer service, and a more competitive information economy. However, while the scale and scope of the data available today bring new, unexpected benefits, they also introduce new and unexpected privacy risks.

In many of these areas, organizations apply de-identification or pseudonymization techniques and measures in order to minimize or eliminate privacy risks to individual data subjects. To de-identify data, those elements which were "personal" because they referred to a particular individual are eliminated. To pseudonymize data, on the other hand, organizations attempt to obscure the connections between individuals and their personal information without completely destroying those connections. As pseudonymous data is therefore still *linkable* to an individual, they pose a slightly higher privacy risk, although still far lower than the risk of unaltered personal data. At the same time, the more that data is manipulated, the less useful and reliable it becomes.

De-identification and pseudonymization enable critical public and private research by allowing for the maintenance and use – and, in certain cases, the sharing and publication – of valuable information sets, even those based on sensitive personal information. However, widespread debate continues to take place over the ways and means, as well as fundamental feasibility, of de-identification. The abundance of Big Data is believed to undermine de-identification efforts through powerful new computing capabilities that can identify data previously considered to be non-identifiable. In many cases, de-identification relies on organizational commitments to keep data from public disclosure and subject to legal or administrative protections, but these promises are often viewed skeptically by critics.

Critics also point to well publicized examples of re-identification, such as the re-identification of individuals from the release of purportedly de-identified AOL Search data, a Massachusetts medical database, or Netflix recommendations. In each of these cases, "Even though administrators had removed any data fields they thought might uniquely identify individuals, researchers . . . unlocked identity by discovering pockets of surprising uniqueness remaining in the data." Given the sophistication of the data handlers in these cases and the repeated success of re-identification attacks, critics conclude that "de-identification fails to resist inference of sensitive information either in theory or in practice."

Defenders of de-identification argue that the attacks were on databases that were not credibly de-identified in any acceptable manner and should not be used to undermine respect for serious de-identification measures. In some cases the debate is over the role of utility of data and relevant risks. Can de-identification that takes into account relevant risks, but not all risks, and that seeks to ensure that the final data set has utility for the intended uses be considered acceptably de-identified? Must every data set (even if held internally) be considered to be a public data set due to potential breaches? Can we trust organizations when they commit to keep data internal or share it only with trusted partners?

If we do not find a way to resolve these questions, we all stand to lose. There are important policy roles for stakeholders working to advance the cutting edge of de-identification science, as well as for those seeking to facilitate the widespread adoption of pragmatic de-identification measures. Furthermore, we must not lose sight of the important role of pseudonymous data in these debates. If de-identification and pseudonymization render data unusable, or are held to impossible standards, we will be denied the socially beneficial activity arising from uses of that data, whether in private or public hands. The ability to distinguish between individuals underlies

many legitimate business and scientific activities in both the U.S. and EU. A black-and-white approach risks both over- and under-protecting personal information, or needlessly sacrificing the utility of data.

The De-Identification Landscape

The Debate

Academics, technologists, regulators, advocacy groups, and businesses have sought for years to establish common standards for the de-identification of personal data. Despite broad consensus around the need for and value of de-identification, the debate as to whether and when data can truly be said to be de-identified appears interminable. The axiom that ‘data can be either useful or perfectly anonymous but never both’ rings louder than ever.²

Rather than discuss *how* to de-identify personal information, the discussion has increasingly turned to *whether* personal information can be (or can be said to be) de-identified. Today, broader policy discussions about de-identification largely fall apart first when attempting to determine what level re-identification risk, if any, is acceptable for data to still be called ‘de-identified’ and second when considering whether or not organizational controls should be considered in that calculus.³ Although technical research into new de-identification techniques remains ongoing, each time a new de-identification solution is proposed another new re-identification risk seemingly raises its head – and then the debate returns whether or not that data can still be properly considered de-identified. This cycle has even led to some researchers contending that all de-identification efforts may be futile.⁴

Policymakers have often sought to draw bright lines around de-identification by simply declaring that certain data can be shared based upon how it has been aggregated and/or its intended use, whether or not de-identification experts agree. In Colorado, the Public Utility Commission has adopted a “15/15” methodology to govern aggregated consumer data. In order to be considered sufficiently protected for public sharing, a data sample must contain more than 15 customers and no single customer’s data may comprise more than 15 percent of the total.⁵ On the other hand, a California utility commission took an approach that weighed the appropriateness of sharing based on who the recipient of the data would be and what purposes it would be used for. Even in the education world, regulators determine whether information has been reasonably de-identified based on whether others in the school community may have additional identifying information. Even HIPAA takes a step down this road, providing that healthcare organizations may deem their data “de-identified” under the Safe Harbor standard by simply removing 17 categories of identifiers from a data file – although it then leaves a catch-all 18th category, unwilling to entirely commit to it.⁶ While having a clear methodological standard eases the compliance burden of de-identifying information, these methods are often criticized by statisticians.

In Europe, meanwhile, a generalized de-identification standard is rooted within the omnibus Data Protection Directive and further clarified by each national data protection authority. The guidance given by the Article 29 Working Party on anonymization has focused primarily on the role of technical de-identification measures, seeking minimal residual privacy risk before determining that data may be considered “anonymous.” While the Working Party cogently presents the technical issues and privacy risks inherent in de-identification, its characterizations of acceptable re-identification risk have been understood by some as requiring near-zero risk,

² Paul Ohm, at 1704 <http://uclalawreview.org/pdf/57-6-3.pdf>

³ Paul Ohm, Broken Promises of Privacy, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006; Cavoukian & Castro, Setting the Record Straight: De-identification Does Work, <http://www2.itif.org/2014-big-data-deidentification.pdf>; Narayanan & Felten, No Silver Bullet: De-identification still doesn’t work, <http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf>

⁴ Is De-identification Sufficient to Protect Health Privacy in Research?, Mark A. Rothstein

⁵ <http://www.cpuc.ca.gov/NR/rdonlyres/8B005D2C-9698-4F16-BB2B-D07E707DA676/0/EnergyDataCenterFinal.pdf>

⁶ “...(R) Any other unique identifying number, characteristic, or code...”

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveridentities/De-identification/guidance.html#safeharborguidance>

an infeasible standard.⁷ EU regulators, too, tend to concentrate on analyzing and applying the highest technical standards available to personal data in isolation, rather than evaluating de-identification measures in light of the practical difficulty of actually re-identifying any particular individual. U.S. regulators emphasize whether an individual's unique identity can be reasonably attributed to them as the locus of de-identification determinations. EU regulators, in contrast, increasingly focus on whether and when an individual can be singled out or treated differently than another individual on the basis of certain information.⁸ If so, that information is deemed personal.

The Framework

Part of the force driving policy discussions into these definitional dead-ends is the inherent value of being able to call data de-identified. As one researcher has put it, anonymization is “ubiquitous, trusted and rewarded by law.”⁹ In the current legal frameworks of both the U.S. and the EU, “personal data” in the EU or “PII” in the U.S. operates as a legal trigger; as soon as data becomes personally identifiable, the full panoply of legal obligations and restrictions applies to it.¹⁰ Accordingly, organizations around the world have structured their internal and external privacy policies around variations of “PII” data – and its converse, de-identified data – locking themselves further into a binary regime.

As Eloise Gratton has previously described, a “literal interpretation of the definition of *personal information* and of the term ‘identifiable’ has in many instances either an over-inclusive outcome, an under-inclusive outcome, or may trigger uncertainty as to which kind of information is in fact “identifiable.”¹¹ While the definition of “personal information” is traditionally intended to be broad, when *any* data may “trigger a system in which organizations and industry players will incur additional costs for complying with [data protection laws],” unintended results arise.¹² In order to provide required privacy disclosures and gather consent for the collection of identifiable information, for example, organizations may be paradoxically forced to actually identify those individuals. Similarly, “it may be difficult for an organization collecting new types of data to grant access if this data has not even been processed.”¹³

Moreover, “it is not always clear at what point a piece of data can be said to be *identifying* an individual”¹⁴ and the legal uncertainty arising from this state of affairs has proven problematic. If neither organizations nor regulators can say whether particular data points are personal, compliance with data protection laws will continue to be suboptimal. There remains significant debate across and within multiple jurisdictions about how identifiability should even be measured, including “whether illegal means that may be used to identify an individual should be considered”; what kinds of costs and resources should be used by an organization to determine if certain data can ‘identify’ an individual and is therefore covered under the definition”; and “whether information should be evaluated alone or in correlation with other information available when attempting to determine if this information is ‘identifiable.’”¹⁵ In addition to shifting legal standards for identifiability, organizations must grapple with changing technologies and information-sharing practices that may increase the likelihood of being able to link data to an identified individual.¹⁶

⁷ See, e.g., Khaled and Cecilia,

<http://idpl.oxfordjournals.org/content/early/2014/12/12/idpl.ipu033.full.pdf?keytype=ref&ijkey=K8xdZaj1rw3EzDx>

⁸ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (The opinion analyzes the robustness of three de-identification techniques on the basis of (i) is it still possible to single out an individual, (ii) is it still possible to link records relating to an individual, and (iii) can information be inferred concerning an individual?) p3.

⁹ http://ico.org.uk/about_us/research/~media/documents/anonymisation_seminar/ohm_slideshow.ashx

¹⁰ Solove & Schwartz, PII 2.0 (and BNA follow-up); Gratton, *If Personal Information Is Privacy's Gatekeeper*

¹¹ Gratton 115 art.

¹² Gratton at 119

¹³ Gratton at 119.

¹⁴ Gratton at 124, citing Bercic & George.

¹⁵ Gratton at 126, 128, 134

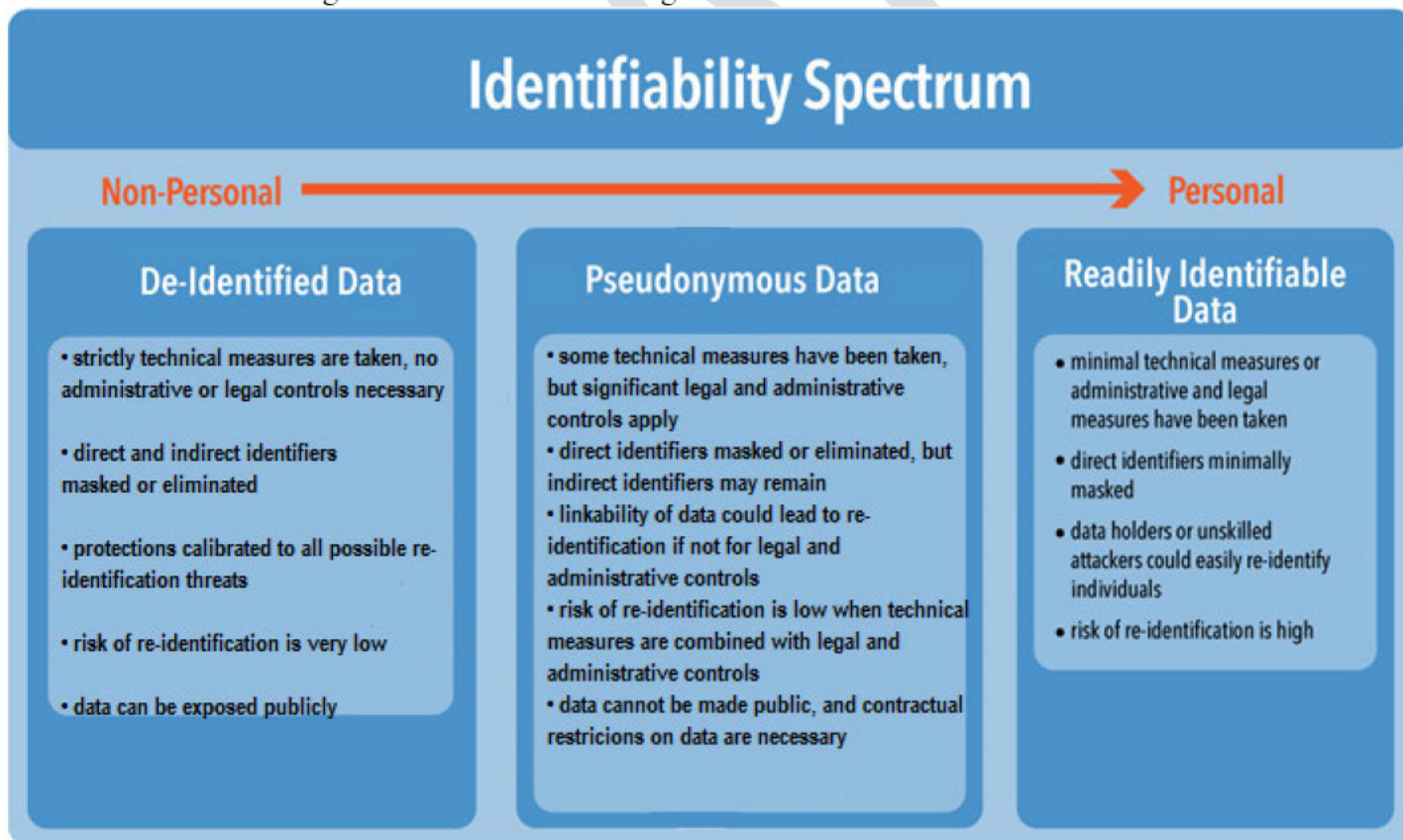
¹⁶ Solove & Schwartz 11-23-12 at 4

Leading scholars have suggested that reforming the current framework to encompass a wider spectrum of data, a so-called “PII 2.0” continuum that instead categorizes data as “identified, identifiable, or non-identifiable.”¹⁷ Depending on the location of data on this spectrum, different legal requirements would apply. Despite wide agreement that this movement away from a binary definition of PII was an accurate reflection of practical reality, policymakers have yet to respond by reassessing current law. While this paper later seeks to demonstrate that, in practice, government and industry standards have started to reflect this sliding scale of identifiability, first it seeks to further develop the stages of this identifiability spectrum.

A New De-Identification Taxonomy

While the rhetorical debate surrounding de-identification rages, organizations continue to employ a range of techniques to de-identify, obscure, and share their data. As these methods offer widely varying levels of protection and obscurity, depending on the context of their use, they have too often become square pegs forced into the round, all-or-nothing holes of the current PII framework. In order to help advance the debate of when data should be properly termed “de-identified,” we have examined this wider range of practices and reclassified data on a spectrum according to its state of identification. A more nuanced understanding of how organizations are protecting their data on the ground will help the entire de-identification community better assess and respond to privacy risks.

The following chart offers the de-identification debate a new taxonomy, categorizing data along a spectrum of identifiability. As described in detail immediately below, data that has been technically manipulated is classified as “de-identified” if it has been rendered non-linkable through the use of technical controls, “pseudonymous” if it is linkable but protected by legal and administrative controls, and “readily identifiable” if it can be easily re-identified notwithstanding minor technical scrubbing of the data.



¹⁷ Id. But see *infra* Part II.

De-Identified Data

At the furthest end of the identifiability spectrum, where data pose the least privacy risk and are considered least personal, are de-identified data. These are data with such low, near-zero privacy risk that they can be shared freely and publicly. In order to create data suitable for public release, statisticians and data scientists seek to apply sophisticated statistical, encryption and other mathematical processes to data sets in order to achieve permanent, impenetrable de-identification.¹⁸ Both direct and indirect or quasi-identifiers are modified in order to protect against future re-identification attacks, and legal and administrative controls are not available. Because these data are to be released publicly, technical protections are the data's last and only line of defense against re-identification attempts. While we leave for others the debate as to whether it is ever appropriate to describe data as "anonymous," it is our opinion for now that the only subset of de-identified data that should be described as "anonymous" is this one, where appropriately applied technical measures render data permanently unlinkable.

De-identification requires an inclusive view of privacy and re-identification risk. Accordingly, these de-identified data are intended to withstand any potential re-identification threats, from world-class external attackers to malicious insiders with existing knowledge of the individuals. When evaluating the effectiveness of a particular de-identification effort, researchers determine whether attackers can identify information about individuals in a certain data set with *any* certainty. If even minimal re-identification is possible, the data is generally not considered to have been acceptably de-identified.¹⁹ This inquiry is enormously useful in moving the science of de-identification forward.

However, in many cases achieving the near-zero re-identification risk sought by technical proponents renders data unusable for the purposes it was gathered.²⁰ Furthermore, limited guidance is available to organizations to determine what level of re-identification risk is appropriate given the value of a particular data set. Because the risks are different, applying the strictest available technical tools has costs if applied in the same way to ordinary business purposes and data used for research on sensitive health topics. An overly strict standard will decrease utility and increase expenses. Critics of some proposed uses of such data may not be concerned about such negative impact, but similar analysis could leave important databases needed for research inaccessible to scientists.²¹ Inflexible confidentiality or consent rules often intended to limit commercial tracking, such as in the proposed European Data Protection Regulation, may inadvertently undermine the utility of cancer and other disease registries, and the critical health research they facilitate.²²

A number of technical methodologies hold great promise to both protect data against re-identification and maintain their utility, but these are not yet broadly feasible. Primary among these is differential privacy, which "ensures that the removal or addition of a single database item does not (substantially) affect the outcome of any analysis."²³ Despite its potential, differential privacy mechanisms do not prevent all sensitive disclosures, require substantial infrastructure investments and sophisticated users, and do not provide the granular data that organizations may sometimes require.²⁴ It has thus have proven difficult for many organizations to employ and has not been widely adopted in practice.²⁵ However, other mechanisms to enable highly perturbed data continue to be deployed in new contexts, as organizations struggle to maximize both privacy and utility. One recent

¹⁸ Khaled; Sweeney; Wu; Narayanan & Felten; Dwork

¹⁹ Narayanan & Felten

²⁰ Gellman note FN 10 (Ohm, citing Brickell & Shmatikov)

²¹ Barth-Jones; Khaled (p 140 "Distortions to the data that produce results that do not make sense erode the trust of the data analysts in the data and act as barriers to the acceptability of the techniques used to protect the privacy of the data.")

²² [http://www.ejcancer.com/article/S0959-8049\(13\)00845-9/abstract?cc=y](http://www.ejcancer.com/article/S0959-8049(13)00845-9/abstract?cc=y)

²³ http://research.microsoft.com/pubs/74339/dwork_tamc.pdf, <http://research.microsoft.com/en-us/projects/databaseprivacy/dwork.pdf>

²⁴ See new Scientific American article on differential privacy

²⁵ <http://research.neustar.biz/2014/09/08/differential-privacy-the-basics/>

example is Google’s application of Randomized Aggregatable Privacy-Preserving Ordinal Response (RAPPOR), a technology that enables anonymously collecting statistics from end-user, client-side software by locally applying privacy-protective randomized response.²⁶

Pseudonymous Data

Moving along the identifiability spectrum we find pseudonymous data: data that is neither fully identified nor fully personal, but that has protected against re-identification by both technical and administrative controls. This data may also be described as obscured, as it has been subjected to some technical modification or masking, albeit without the same technical rigor as de-identified data. Importantly, a combination of technical and administrative protections must achieve a sufficiently *low* risk of re-identification. In the EU, this data is considered personal, but may weigh in favor of data processing during the legitimate interests balancing test. In the U.S., if it is protected by sufficient administrative and legal controls (presuming reasonable technical measures exist), it is considered not personal.

Data that are *not* intended for public disclosure do not necessarily need to be subjected to the same stringent technical measures as data in the previous category to ensure re-identification risks remain low. And because these data will not be released to the entire world, technical measures are not the sole line of defense against re-identification: instead, legal and administrative controls can be used to minimize any residual privacy risk. Therefore, organizations may be able to use less data-destructive technical measures, supplemented by stricter administrative and legal controls, to achieve a sufficiently low risk of re-identification.

Pseudonymization spans a wide range of practices, and requires legal and organizational protections (such as contractual promises not to re-identify data or segregating personal and non-personal data) in order to be relied upon. It may include data that is: only temporarily de-identified; masked by weaker technical applications;²⁷ protected against some credible threats but not others; or that is maintained in a manner that is obscured, but could be easily identified by the holder of the data, if legal or policy commitments are ignored. The critical distinction is that while direct identifiers are removed or manipulated just as they are for de-identified data, pseudonymization does not technically mask indirect identifiers, or relies on administrative measures (which may be bypassed) to de-link indirect identifiers from data subjects. Thus, data is not obviously or easily linked to an individual, but does remain *linkable*. Because of this, pseudonymous data should not be released publicly, and additional contractual safeguards may be needed before such data can be shared.

Accordingly, risk assessments for pseudonymous data may be conducted more pragmatically, focusing not on the every possible attack vector but instead on those that are truly feasible or likely to be available to an attacker. This more narrowly risk-based assessment²⁸ thus considers re-identification risks “in the particular circumstances involved, having regard to such factors as the motives and capacity of the organization or individual to re-identify the information.”²⁹ As well as the practical risk of an attack, other considerations may include the sensitivity of the data and the risk of harm if an attack is successful. By focusing their de-identification efforts on realistic threat models, organizations can more easily employ and assess the technical mechanisms available to them to in order to find the best fit for their particular purposes.

Furthermore, pseudonymous protections can be calibrated on a case-by-case basis to protect against a wide range of likely re-identification threats, both internal and external. Administrative and legal controls are particularly effective against unskilled or opportunistic re-identification, such as by peeping employees or vendors, with contractual agreements providing both deterrents to and punishments for re-identification. Even

²⁶ <https://static.googleusercontent.com/media/research.google.com/en/us/pubs/archive/42852.pdf>

²⁷ Such as constraining names, adding noise, character scrambling, character masking, truncation, or encoding. Khaled 164-66.

²⁸ Khaled book

²⁹ Cavoukian & Khaled June 2014

inadvertent re-identification – such as when a researcher accidentally recognizes a family member in a data set – can be protected against through administrative measures, such as automating data processing so that no human interacts with it; utilizing non-persistent data; or shifting data processing to another country, where the risk of accidental recognition is significantly decreased.

By working with a risk-based approach, organizations can be more precise in calibrating the balance between protecting privacy and preserving utility with their data sets. As a result, this has proved particularly fertile ground for the development of new de-identification techniques. One of the most well-known tools for practical technical de-identification is the Privacy Analytics Risk Assessment Tool (PARAT) developed by Dr. Khaled El Emam, which “de-identifies information in a manner that simultaneously minimizes both the risk of re-identification and the degree of distortion to the original database.”³⁰ Another innovative technical approach to de-identification is the Anonos “Dynamic Data Obscurity” method, which “dynamically segments de-identifiers to data stream elements at various stages” causing data to undergo a physical transformation so data is no longer identifiable to third parties without assistance from the user to which data pertains while still preserving full access to all underlying data.³¹

Many organizations use the term ‘de-identified’ or ‘anonymous’ for this type of data because it does require credible steps to hide individuals’ identities be taken. Pseudonymization techniques might preserve the utility of data better than de-identification techniques, for example, and still render quite low re-identification risk. In addition, explicitly describing this data as personal might limit an organization’s ability to use and share it, even for non-commercial or legitimate purposes. There are any number of uses for data that do require the information to be linkable and to include a significant number of historic details, within both the corporate and scientific spheres. For instance, key-coded data, in which personal data “have been stripped of direct identifiers and replaced by a key to avoid unwanted or unintended re-identification” by anyone without the key, only a limited remains indirectly identifiable even when backed by robust administrative safeguards securing and limiting access to the key.³² The ability to link research data to individual data subjects may be necessary during clinical trials, for example, to enable treatment if a researcher discovers that follow-up medical attention is required.³³ Key-coded data is used extensively in a range of sectors where limited re-identification may become necessary or desirable under special circumstances, including pharmaceutical research, scientific and historical research, marketing analysis, and online and mobile services.³⁴

Readily Identifiable Information

Finally, the furthest end of the spectrum contains data that has been only superficially manipulated or released in a manner where it could be readily and easily linked to an individual. Even if such data does not explicitly identify an individual, or some minimal administrative or legal controls are present, if the risk of re-identification is *high* then data should not be considered pseudonymous. Data that are personal in some context (e.g., nine unique digits comprising a social security number) or that are have been linked to an identifier only temporarily may fall within this category, as they may be marginally protected when taken out of context but remain vulnerable to any minimally intensive re-identification effort. In most cases, this data should be considered explicit PII, subject to the full complement of data protection laws.

³⁰ Cavoukian & Khaled June 2014 (p 13), also <http://www.privacyanalytics.ca>

³¹ Gary LaFever, IAPP Privacy Perspectives article (Oct. 20, 2014) available at <https://privacyassociation.org/news/a/what-anonymization-and-the-tsa-have-in-common/> and comments to FTC and Mauritius DPC officials available at <http://www.anonos.com/anonos-enabling-bigdata/>

³² http://www.epag-thinktank.eu/docs/whitepapers/EPAG_Whitepaper_Key_Coded_Data.pdf

³³ <http://www.cov.com/files/Publication/26174ea1-6641-457f-990c-f874b10f7670/Presentation/PublicationAttachment/350459db-4a73-4ac4-b59a-fa8f354473ee/oid64167.pdf>

³⁴ http://www.epag-thinktank.eu/docs/whitepapers/EPAG_Whitepaper_Key_Coded_Data.pdf (find substitute source)

A Path Forward: Expanding the Framework

The current binary policy view has led to an impasse where researchers and organizations make increasing uses of that data in formats they consider acceptably and pragmatically de-identified while policymakers seek to ensure that the same data falls within the scope of data protection laws. And yet, as Paul Ohm writes, “[n]o matter how effectively regulators follow the latest re-identification research, folding newly identified data fields into new laws and regulations, researchers will always find more data field types they have not yet covered. The list of potential PII will never stop growing until it includes everything.”³⁵ In order to help bridge the gap, we propose a new framework that will more granularly categorize data along the spectrum of identifiability, allowing organizations to more accurately reflect their efforts to de-identify, pseudonymize, or otherwise protect data and ensuring that policymakers on either side of the de-identification debate no longer simply speak past each other.

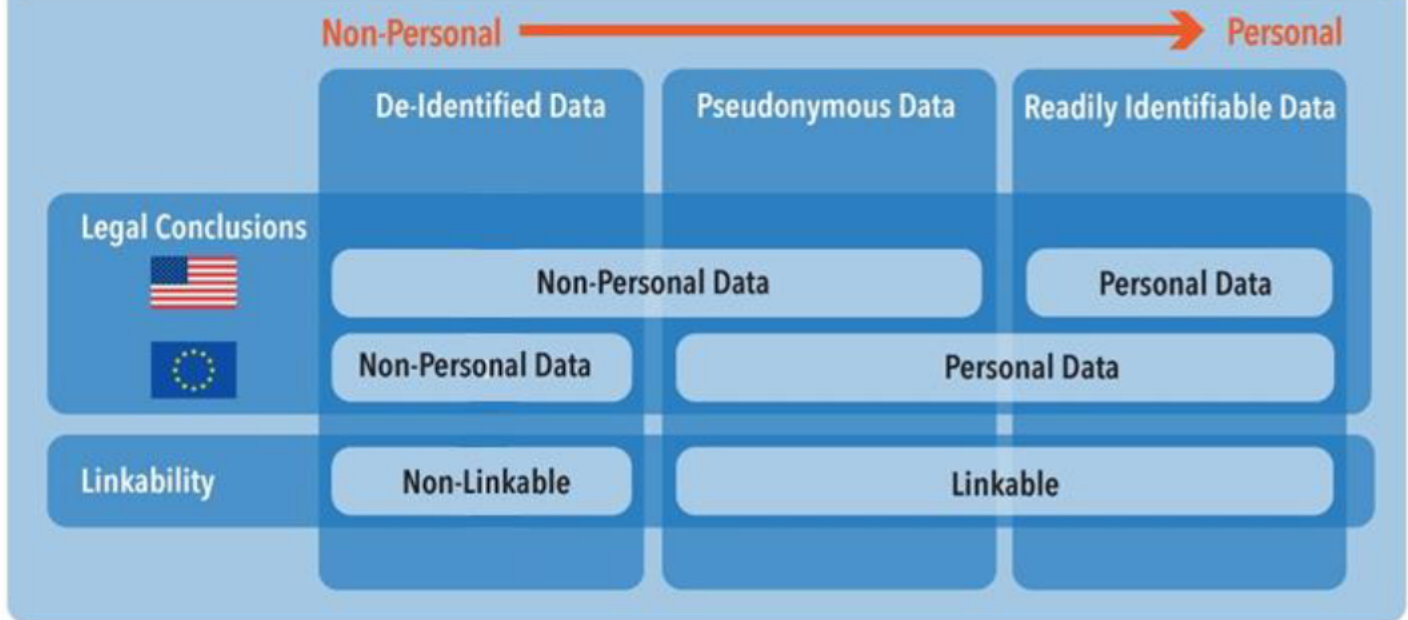
As we described above, we believe that there already exists a wider range of obscured or “de-identified” data than is conceived of by the current PII framework. Rather than distort these practices – and the threat and utility models underlying them – by forcing them into either “identified” or “de-identified” pigeonholes, we suggest introducing more flexibility to the PII framework by recognizing a spectrum of de-identification practices.

Accordingly, we propose that “de-identified” terminology be reserved for data that cannot be linked to a particular individual because of the elimination of direct and indirect identifiers through comprehensive technical controls. This data would be considered *non-personal* and exempt from data protection regulations. It would be freely shareable. Next, “pseudonymous” data, in which direct but not indirect identifiers are removed and administrative or technical measures reduce re-identification risk to “low,” would be considered personal in some circumstances and non-personal in others. This data could never be made public, and, as described below, would often be subject to some, but not all, data protection requirements. Finally, data in which direct but not indirect identifiers are only nominally masked, administrative or legal controls are negligible or non-existent, and where the risk of re-identification is high would be considered “readily identifiable” and considered *personal information*, subject to all relevant data protection laws.

Mapping the expanded data taxonomy to the PII framework produces the following chart, which describes each data category in terms of its ‘linkability’ and legal status under U.S. and EU law:

³⁵ Broken Promises of Privacy, 57 UCLA L. Rev. 1701, 1742 (2010).

Identifiability Spectrum



The inclusion of pseudonymous data in this spectrum presents our most significant break with the current PII framework. This data is a conundrum in that it often does mask the data subject's identity, but not always reliably enough to establish a guarantee of re-identification against a determined technical attacker. With additional legal and administrative controls, however, the actual risk of identification can be minimal. Subjecting pseudonymous data to the full set of Fair Information Practice Principles, however, could perversely incentivize organizations to maintain the data in a *more* identified manner. For example, an organization that would otherwise maintain data in a pseudonymous state (thus decreasing privacy risk) might be required to re-identify the individual in order to comply with the individual's statutorily mandated access right to the data. In many other cases, including critical medical and social research projects, explicit consent requirements or a restriction on sharing would completely eliminate the utility of the data.

Our framework addresses this dilemma by proposing that pseudonymous data be subject to some, but not all, data protection requirements, in proportion with the risk of re-identification and the nature of the data. Depending on the totality of the circumstances, pseudonymous data could be subject to a range of increasingly intensive legal elements, such as consent, data minimization principles, sharing restrictions, use limitations, or other important privacy protections. Within this framework, data that is more personally identifying or that faces greater re-identification risks (such as location records) would be subject to certain set of privacy-protective standards (such as technically rigorous pseudonymization, or opt-in consent). Data that is less identifiable or that is less likely to be attacked, however, would be held to correspondingly less intensive standards (such as opt-out consent, or increased reliance on administrative controls). An organization's evaluation of the risks and benefits of processing data in particular ways may include an obligation to err on the side of privacy over utility as the risk of attack and the risk of harm increase.

Pseudonymous data naturally encompasses a diverse range of data, with correspondingly diverse threat models to be protected against and potential uses to support. Organizations must therefore be careful in assessing the default privacy protections applicable to a particular data set and the fairness of a particular use. In order to ensure that the claimed benefits of a particular use are appropriately weighed against its potential privacy risks,

we have previously proposed that organizations engage in Data Benefit Analysis (DBA).³⁶ A complement to the traditional Privacy Impact Assessment (PIA), the DBA assesses such variables as the “nature of the benefit, the identity of the beneficiary and the likelihood of success” and feeds the results into existing PIAs in order to craft “a balanced, comprehensive view of big data risks and rewards.” This process recognizes that, in some circumstances, a small amount of privacy risk may be worth accepting if the ultimate result will lead to much larger benefits. A DBA allows organizations to rationally measure the potential benefits to consumers and society at large that will arise out of using personal data in a particular way, in order to then determine whether those benefits outweigh the privacy risks also arising from it.³⁷

It is important to note that re-identification risk is not determined solely on the type of controls utilized, or the type of data to be protected, but rather by a combination of case-specific factors and threats. There may be circumstances in which non-sensitive data is adequately protected by pseudonymization, just as there may be circumstances when more comprehensive de-identification measures are required. However, by making it more clear externally by what criteria data is considered de-identified,³⁸ organizations will be able to debate the sufficiency of their measures on fair ground. Rather than engage in a false debate about whether data is capable of being re-identified under any circumstances, discussions can then turn to whether the data has been appropriately de-identified based on the risk of re-identification, the safeguards in place, and the potential benefits of preserving a particular amount of utility in the data.

Relevance to the FTC Framing of PII

As Big Data and increasingly interconnected technologies continue to strain existing privacy norms, legislators and regulators have already begun exploring how to re-draw the lines between personal and non-personal. In the U.S., the FTC has acknowledged the broad consensus that “the traditional distinction between PII and non-PII has blurred and that it is appropriate to more comprehensively examine data to determine the data’s privacy implications.”³⁹ In order to address such concerns while still imposing some practical limits, the agency crafted a new PII standard, considering data personal when they are “reasonably linkable” to a particular consumer or device. At the same time, the FTC described three steps organizations can take to minimize such linkability, and thus their liability. Accordingly, the FTC considers data to be *not* “reasonably linkable,” or de-identified, if an organization 1) takes reasonable measures to ensure that the data is de-identified, 2) commits publicly to maintaining and using the data in a de-identified fashion, and 3) contractually prohibits downstream recipients of the data from attempting to re-identify it.

While the FTC’s definition nominally still creates a linkable/non-linkable binary, it nevertheless captures many of the same factors embodied in our proposed categorization. Rather than holding all anonymous data to the highest technical standard, the FTC’s approach recognizes the importance of administrative and legal protections when used in combination with reasonable, technical de-identification measures. The FTC’s approach also acknowledges the significance of contextual factors in determining re-identification risk, noting that “what qualifies as a reasonable level of justified confidence depends on the particular circumstances, including the available methods and technologies. In addition, the nature of the data at issue and the purposes for which it will be used are also relevant.”⁴⁰ Again, this recognition that different types of data may be more

³⁶ http://www.futureofprivacy.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf

³⁷ As the Article 29 Working Party noted, “the very nature of the right to the protection of personal data and the right to privacy . . . are considered relative, or qualified, human rights. These types of rights must always be interpreted in context. Subject to appropriate safeguards, they can be balanced against the rights of others.” Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

³⁸ E.g., X set of sensitive data is being considered de-identified because it has been subjected to stringent perturbations and some administrative restrictions, while Y set of data is being considered de-identified because it is non-sensitive, direct and quasi-identifiers have been masked, and substantial legal and administrative controls exist on its use and sharing.

³⁹ Era of Rapid Change (2012)

⁴⁰ FTC Era of Rapid Change at 21

sensitive, or more at risk, or otherwise merit different levels of protection – particularly in the liminal zone between “reasonably linkable” and “non-linkable” – directly parallels our taxonomic approach.

One aspect of the FTC’s definition of “reasonably linkable” requiring further discussion is the inclusion of data that identify devices rather than identifiers. The agency’s current guidance simply indicates that data is personal to the extent it identifies “an individual *or device*,” without further elaboration as to why or when any given device is assumed to belong to an identifiable individual.⁴¹ Certainly many devices are used by only one individual, who may be readily identifiable, but not all. Some devices may be shared equally between two people, or ten, or more. In today’s Internet of Things environment, many devices maybe part of an ecosystem and have no connection to any individual. Identifiers, including those that identify devices rather than users, come in a wide variety of formats and features; whether any particular device can be reasonably traced to an individual requires a case-by-case assessment, not a blanket assumption that all devices as personal. For example, some identifiers have look-up databases in the hands of the organization holding the data, while others have public look-up databases, creating two different levels of re-identification risk. Another identifier might be easily cleared by its users, although others could be hard-coded, or only clearable by resetting the entire device. And yet another identifier might only be used locally, while others are shared globally. All of these factors need to be accounted for in assessing the risk of re-identification

Despite the FTC’s broad definition of personal data as incorporating reasonably identifiable devices, their enforcement actions reflect a more nuanced recognition that some identifiers create more privacy risk than others. For example, in its consent decree with Myspace, the agency emphasized that privacy concerns arose from the sharing of quasi-identifiers when there existed a publicly available look-up directory, which could be used to actually re-identify an individual, rather than from the transmission of the pseudonymous device identifier itself. This more nuanced and risk-based application of privacy rules to quasi-identifiers is also reflected in some U.S. courtrooms. For instance, a California court examined Hulu’s unique User IDs “very practically” and determined a unique quasi-identifier, without more, is not PII under the VPPA. When that court examined Hulu’s use of the Facebook “Like” button, which transmitted cookies containing unique Facebook IDs, however, it did find a violation of the VPPA, as “the link between the user and the video was more obvious.” Given the wide variation that can exist in identifiers, treating all “device identifiers” the same under the letter of the law does not provide a useful framework for organizations, nor does it take into account the particularized risk of identification arising from each identifier.

While we agree that persistent or universal pseudonyms should generally be subject to more robust set of privacy protections than truly un-linkable data, we do not agree that they should be considered *per se* linkable, or fully personal. Instead, identifiers – whether they arise from a device or not – that are pseudonymous, subject to administrative controls and appropriate consumer protections, could be considered de-identified data in many cases. The more globally unique an identifier is, or the more clearly individual it is, or the more parties that can access it, the more private it should be treated. Identifiers that are only readable by one organization, or that are controllable by a consumer, or that can be shared between consumers, on the other hand, could reasonably be considered less private and subject to less stringent protections.⁴²

Relevance to the EU Framing of PII

In Europe, too, the traditional definition of PII may soon see an official shift. The current European Data Protection Directive regulates information relating to a natural person who is “identified or identifiable,”⁴³ taking an inclusive approach in extending data protections to its people and their quasi-identifiers. Currently, only data that has been irreversibly de-identified and protected against “all the means likely reasonably to be used” by either the data controller or a third party can be considered de-identified.⁴⁴ However, European

⁴¹ Id, emphasis added.

⁴² See also <https://www.cdt.org/files/pdfs/CDT-Pseudonymous-Data-DPR.pdf>

⁴³ http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

⁴⁴ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

regulators, courts, and advisory groups have struggled with the concept of “identifiable” data for years.⁴⁵ Over the course of three years, for example, five French courts and the CNIL took contradictory positions on whether or not IP addresses were personal information.⁴⁶ European courts have not yet reached a consensus on how to determine if a particular type of data was personal.⁴⁷ Despite these struggles, it remains possible that pseudonymous data could appear in the final Data Protection Regulation in some form. Given the importance of pseudonymized data to a wide range of societally and individually useful purposes, it will be important for the final GDPR to include a definition of pseudonymous data and appropriate measures of protections and permissions when data is pseudonymized.

Pseudonymous data of the type we describe above, while protected by both technical and administrative controls, would still be considered *identifiable* and thus personal for the purposes of EU law. However, in keeping with our proposed framework, pseudonymous data could be a key factor to consider in assessing how EU data protection obligations apply. For example, we would propose that pseudonymous data could carry a rebuttable presumption that data processing is legitimate and that pseudonymization could be deemed a compatible use with regards to the purpose limitation principle. As existing EU data protection laws set the bar to de-identification higher than many countries, adding a “middle ground” to EU data protection laws would encourage not only more useful research, it would encourage the adoption of more reliable (albeit not technically perfect) technical and administrative controls.

Other rules to incentivize the creation and use of pseudonymous data have already been proposed both by EU member delegations and interested policy organizations.⁴⁸ As we have suggested previously, we believe that “pseudonymization should excuse controllers from certain obligations under the GDPR, such as obtaining explicit data subject consent or providing rights of access and rectification.”⁴⁹ Others have similarly urged that “a general requirement that consent be ‘explicit’ is reasonable, but that for some categories of data, the ‘legitimate interest’ justification paired with a robust right to refuse processing is appropriate.”⁵⁰ Previous drafts of the GDPR text have also suggested that controllers could be rewarded for utilizing pseudonymous data, as such processing could be presumed not to significantly affect the interests, rights or freedoms of the data subject.⁵¹ One of the most repeated recommendations has been that “for unauthenticated pseudonymous data sets, it also be reasonable to excuse data controllers from obligations such as access rights and data portability.”⁵²

Furthermore, the legitimate interest analysis under Article 7 of the existing Data Protection Directive harmonizes with the risk analysis underlying both the U.S. approach to the use of pseudonymous data and our proposed framework above. The legitimate interests balancing test represents a fundamental recognition that privacy interests and data utility should be weighed together in certain circumstances.⁵³ The Article 29 Working Party has made clear that the application of appropriate measures “could, in some situations, help ‘tip the balance’” in favor of the data controller’s legitimate interests. Pseudonymization and personal data that are “less directly and less readily identifiable” are specifically mentioned as one such “less risky form[] of personal data processing,” wherein the general likelihood of “data subjects’ interests or fundamental rights and freedoms being interfered with is reduced.”⁵⁴

⁴⁵ Gratton p 126

⁴⁶ Id p 126

⁴⁷ Id 127, conflicting case law

⁴⁸ <http://www.futureofprivacy.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-De-Id-January-201311.pdf>, CDT paper, leaked 2013 draft

⁴⁹ <http://www.futureofprivacy.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-De-Id-January-201311.pdf>

⁵⁰ CDT paper

⁵¹ <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN>

⁵² CDT, but also draft *id* and Jules-Omer paper.

⁵³ WP29 on legitimate interest processing

⁵⁴ Id. At 43

In order to further incentivize the use of pseudonymous data in Europe, we would urge policymakers to extend the legitimate interests test to not only personal and pseudonymous Article 7 data, but also to appropriately safeguarded and pseudonymized special categories of data under Article 8. Under this approach, if data of any sensitivity could be shown to have been subjected to credible pseudonymization, with sufficiently low risk of re-identification, then it would be permitted to undergo the balancing test. This is not at all to say that all uses of pseudonymized sensitive data would automatically be deemed legitimate, simply that there would be an opportunity to assess and balance “the legitimate interests of the controller, or any third parties to whom the data are disclosed, against the fundamental rights of the data subject.”⁵⁵ The processing of pseudonymized health data for healthcare research or healthcare device maintenance, for example, may result in a different balance of interests than the processing of that same data for marketing purposes. That some uses of pseudonymized sensitive data may not pass the legitimate interest test does not mean that other, more compelling uses for that data should be thrown out like the proverbial baby in the bathwater.

It will be essential for the EU to have a pseudonymous category that allows the use of such data, or many standard and essential data uses will exist in an area of uncertainty. As we explain in the next section, organizations operating in Europe already operate under such uncertainty, finding their uses and protections for pseudonymous data subject to the views of individual DPAs.

PII 2.0 in Practice

While proponents of PII 2.0 models have urged policymakers to officially expand the PII framework, these efforts have yet to be reflected in the laws. Re-categorizing data may increase the precision of the de-identification debate, but without a framework that addresses the middle ground (i.e., pseudonymous data), de-identification in practice will remain strained. We argue, however, that the gap in real world application of these concepts is less than it appears on paper.

Outside the de-identification debate, we are already beginning to see an implicit recognition that certain states of data warrant different protections. As this approach gains broader recognition, we hope that it will provide a model for organizations and regulators to begin explicitly recognizing intermediate data states and assigning them tailored protections, further clarifying the divide between intermediate, identified and de-identified data. For these intermediate data sets, it must be clear that privacy restrictions do apply. In some cases consent may be required, or retention policies or commitments not to use data in certain discriminatory ways, or even notice or certain limited access. While regulators have been opaque in their application of such distinctions so far, the underlying logic to various recent decisions reflects this approach.

Indeed this has often been the case in the application of EU law, where regulators describe data sets such as web logs as personal, but then recognized the need for certain protections but not others. For example, German data protection authorities in Hamburg passed a resolution in 2009 that made the analysis of user behavior, based on the personal linkage of these data by using their full IP address, only permissible with the user’s deliberate and explicit consent.⁵⁶ Most web analytics services, which gather such information as a matter of course, did not have practices in place to gather such consent, violating the new law. Rather than oust the service entirely, the DPA instead entered into a binding resolution with Google in 2011 implementing certain – but not all – of the law’s protection measures. These included allowing users to opt-out, allowing website operators to request that IP addresses collected be ‘anonymized’ (by deleting the last digits) and requiring data processing agreements between Google and website operators using its Analytics. Website operators were also required to inform users about the use of Analytics in their privacy policies, including notice of the opt-out, and to delete data collected using previous, non-compliant analytics profiles.

⁵⁵ Id. At 3.

⁵⁶ <http://www.iitr.us/publications/20-hamburg-data-protection-authority-data-protection-conforming-use-of-google-analytics.html>

In Canada, the risk-based model is likewise in sync with this argument. Applying certain privacy protections to certain sets of data is perhaps most obvious in the increased obligations applied to sensitive data, as compared to non-sensitive data. For example, in January 2014, the Office of the Privacy Commissioner entered into a settlement with Google regarding retargeting of advertisements based on an individual’s health-related searches. Canadian privacy law generally considers information collected for the purpose of online behavioral advertising to be personal information, and requires only implied consent from the consumer (an opt-out); however, sensitive information is treated differently, and requires express consent (an opt-in). In response to the complaint, Google agreed to increase its oversight of advertisers’ remarketing campaigns and use of sensitive data.

Similarly, in the U.S. self-regulatory models for behavioral advertising and the Mobile Location Analytics (MLA) Code developed by the Future of Privacy Forum already bind a number of organizations to this approach. The National Advertising Initiative (NAI) Code of Conduct, for example, sets obligations for notice, choice, opt-out, and non-discrimination on data sets that are defined as “non-personal” – that is, neither anonymous nor personal – by their codes.⁵⁷ Sensitive data also require opt-in consent when used for interest-based advertising. The DAA Self-Regulatory Principles also set protections for pseudonymous identifiers, determining that “data is not considered PII under the Principles if the data is not used in an identifiable manner.”⁵⁸ Here, an IP address is *not* PII when collected in isolation (and thus does not require consent or transparency when used for online behavioral advertising), but it *is* PII subject to the full set of Principles when it is “in fact linked to an individual in its collection and use.”⁵⁹ The MLA Code, on the other hand, requires its organizations to provide in-store notice, to hash mobile device ID MAC addresses and to set discrimination and retention limits around a non-personal but not de-identified set of “de-personalized” data.

If one examines their behavior, rather than their rhetoric, then, it appears that policymakers have long accepted a more sliding-scale understanding of PII, considering some intermediate state data personal but not requiring all of the elements of the law be applied to it. Similarly, even as organizations continue to claim that intermediate state data is de-identified or non-personal, they apply significant privacy requirements to it, including notice, choice, anti-discrimination provisions, retention limits, and more.

Critical Factors for a Successful De-Identification Framework

In order for structural changes to the de-identification and PII framework to be meaningful, the de-identification debate needs to be grounded in more nuanced terminology and de-identification practices need to be more transparent.

Transparency

Much of the current de-identification debate has been dedicated to strawmen, with both sides talking past one another about what is or is not de-identification in what has become a zero-sum discussion. In order to advance de-identification policy – and earn consumers’ and regulators’ trust – organizations need to be more transparent about what data they maintain, how it is used, how it is protected and what threats it is protected against. Critics and concerned consumers will not be satisfied with vague promises of “anonymity.”

If data is claimed to be anonymous or de-identified, organizations should make clear by what standard they have made that determination, to aid others in understanding both the possible utility of the data and the possible threats to it. While security and trade secret rationales may prevent organizations from disclosing the exact details of their technical safeguards or administrative and contractual requirements, organizations could still describe the types of protections they have instituted. Within our above framework, an organization that

⁵⁷ (although many participating organizations claim anonymity for such data)

⁵⁸ <https://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf>

⁵⁹ Id.

describes its data as “pseudonymous” should be able to inform consumers if or when, for example, it key-codes their personal information, trains its employees on privacy and security, or relies on contractual agreements to prevent onward sharing of data. Another organization, describing its data as “de-identified” and suitable for public use, could describe to consumers in plain language that it has utilized highly technical measures to remove or perturb both direct and indirect identifiers so that they are no longer linkable to the data, but that no further administrative controls have been utilized.

While organizations should be transparent about the method of de-identification and administrative controls they have in place, those must also be backed up by legal force. Increased transparency, in the form of public statements or representations about if and how data has been de-identified, also creates accountability. In the U.S., public promises regarding privacy are enforceable by the Federal Trade Commission under Section 5 of the FTC Act, while in Europe national Data Protection Authorities can and will continue to investigate and enforce such notices under the DPD and the proposed GDPR. Without increased transparency, industry standards and best practice guidance will not develop and debates about what de-identification is will stop us from realizing what it could be.

In order to build a framework in which de-identification encompasses both the technical frontier of de-identification science and more pragmatic technical measures, administrative controls and commitments not to re-identify data must be strictly enforced. And in order for pseudonymous data to be accepted, there must be a shared understanding of what administrative or legal measures are and should be buttressing data which are linkable, but not linked, to individuals, so that they can be utilized productively without undue re-identification risk. To help accomplish these goals, it is important that measurable standards be adopted so that de-identification and pseudonymization practices can be assessed and meaningful certifications can be published.

Terminology

As we discussed before, there are a range of reasons why the current terminology has been overused, and why organizations have stretched “anonymous” to cover a wider range of practices. We propose that, by a consistent terminology to describe how data is de-identified and protected, organizations can be more transparent about what they are doing; researchers can more accurately evaluate real-world re-identification risks; and regulators can better tailor their activities and guidance to strike the correct balance between protecting privacy and preserving the utility of data. Not only must data be categorized consistently, those categorizations must be able to accommodate new discoveries and advances by data scientists and re-identification specialists. In keeping with this approach, we propose recognizing a spectrum of de-identified data; pseudonymous data; and readily identifiable data.

Before we can turn to the debates of real importance in de-identification around the efficacy of de-identification data sets that have had rigorous de-identification methodologies applied, we must first cut through the confusion surrounding it. Both sides of the debate should work together to increase transparency around what efforts organizations can and do undertake to protect data and what protections are really being utilized. This need to find common terminology will not be an isolated event, accomplished once and then set aside. What we mean by technical de-identification and pseudonymization will necessarily change over time, as the techniques that are capable of de-identifying, or even re-identifying data, will continue to evolve. The terminology should stay the same, but the specifics of how such techniques are applied will change with technological advances. Consistency and clarity between stakeholders as to what they mean when they say ‘de-identification’ will be critical in ensuring that de-identification policy can continue to progress.

Next Steps

It is clear that we need a fundamental shift in public de-identification policy debates, both in terminology and approach. Rather than continue to debate whether data is or is not personal or de-identified, discussion and

policies must move towards a more nuanced approach to data that embraces the reality of varying risks of re-identification as well as acknowledging the risks and benefits of different uses of data. Data can exist in different states, subject to different threat models and better suited to different sets of protections or subject to different risks.⁶⁰ By re-examining terms like “de-identified” and “pseudonymous,” and using them only in very clear and defensible circumstances, we believe that appropriate protections could be found to preserve both utility and privacy along the whole spectrum of personal information.

Once we have left the binary identified/de-identified model, we can begin deciding what the rules should be for pseudonymous data and building tools to support them. Data that is intended to for public release, for example, requires the strongest technical de-identification measures, as it “provides the sole line of defense protecting individual privacy.”⁶¹ Depending on what the data is to be used for, this may mean applying differential privacy tools to add noise to the dataset; scrubbing or aggregating certain fields; or hashing, salting or key-coding inputs and imposing additional administrative safeguards to buttress those techniques.⁶² For data intended only for internal use, or more limited sharing, less invasive de-identification techniques may suffice when buttressed by administrative and legal controls, with those controls becoming more comprehensive as the risk of re-identification rises. Standard controls may include robust data security and use policies; access limits; employee training; data segregation guidelines; data deletion policies; individual access and correction rights; contractual limits on third parties’ access, use, and sharing of data; penalties for contractual breaches; or auditing rights on service providers or business associates. A full examination of such controls is beyond the scope of this paper, but for additional details a technical paper is forthcoming.

Conclusion

Currently, a legacy legal structure is straightjacketing policy in this area by insisting on a binary identified/de-identified categorization of data and all-or-nothing privacy protections. This binary categorization has found its way into some legal models, including proposals for the next generation of privacy and regulatory oversight under the draft European General Data Protection Regulation.⁶³ In its place, we need to develop new models recognizing a spectrum of data states with varying restrictions and protections based on the actual utility and threat risks to that data. To do this, we must first recognize the full spectrum of data, from identified to de-identified and everything in between, as it already exists in practice. Only once we have reframed the debate can we develop legislative models that reflect the relevant choices and protections that should attach when data is less than personal.

⁶⁰ Swire, Practical Obscurity and Practical De-Identification: A Typology of Levels of De-Identification (forthcoming)

⁶¹ Lagos & Polonetsky, Public vs. Nonpublic Data

⁶² Omer & Jules, Seeing the whole spectrum paper

⁶³ Should the proposed GDPR adopt a pure binary requirement, it risks getting ahead of this important debate.

[REDACTED]

From: [REDACTED]
Sent: 24 September 2015 12:59
To: [REDACTED]
Cc: [REDACTED]; [REDACTED]; D'CUNHA Christian
Subject: RE: Meeting request on behalf of Ms [REDACTED] and Mr [REDACTED] - General Electric

Dear Ms [REDACTED],

Thank you for your e-mail.

The meeting on 29th September at 11.00 is confirmed now with the attendees in your previous e-mail.

Please do not hesitate to contact me should you require any further information.

Kind regards,

EA to [REDACTED]
PA to [REDACTED]



T +32 [REDACTED]
F +32 [REDACTED]
M +32 [REDACTED]

E [REDACTED]
www.ge.com

General Electric (GE)
2-4, Rond Point Schuman
1040 Brussels, Belgium

From: [REDACTED]
Sent: Thursday, September 24, 2015 12:42 PM
To: [REDACTED]
Cc: [REDACTED]; [REDACTED]; D'CUNHA Christian
Subject: RE: Meeting request on behalf of Ms [REDACTED] and Mr [REDACTED] - General Electric

Good morning,

Mr Buttarelli will be very pleased to meet the GE delegation on 29 September at 11.00 but due to other commitments he can stay about 30 minutes.

So from your side there will be:

- Mr. [REDACTED], [REDACTED] - [REDACTED]
- Ms. [REDACTED], [REDACTED] - [REDACTED]
- Mr. [REDACTED], [REDACTED] - [REDACTED]

I would need your confirmation as I should as for the permission access to the building.

Kind regards,



[Redacted]
Administrative Assistant
☎ (+32) [Redacted] | 📠 +32 [Redacted] | 📧 MTS [Redacted]
Email [Redacted]
European Data Protection Supervisor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels
🐦 @EU_EDPS 🌐 www.edps.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

From: [Redacted]
Sent: [Redacted]
To: BUTTARELLI Giovanni
Cc: [Redacted]; [Redacted]
Subject: Meeting request on behalf of Ms [Redacted] and Mr [Redacted] - General Electric

Dear Mr Buttarelli,

With the occasion of the visit of Mr. [Redacted] ([Redacted] of General Electric) in Brussels, we would like to request a meeting with you in the week of September 28th.

Since the last meeting with your office, we note the progress made on the General Data Protection Regulation but also the general engagement of the European Union to maximize the potential of the Digital Economy while safeguarding privacy and the protection of personal data. Our company being a leader in bringing together the physical and digital worlds and inventing the next industrial era in a variety of businesses, we believe this is a good moment to continue the dialogue with your office on these topics.

Attendants from GE will be:

- Mr. [Redacted], [Redacted] - [Redacted]
- Ms. [Redacted], [Redacted] - [Redacted]
- Mr. [Redacted], [Redacted] - [Redacted]

Could you kindly suggest the dates and times that would be most convenient for you for a meeting within the week of 28th September?

We thank you in advance and look forward to meeting you.

Best regards,

[Redacted]
PA to [Redacted] - [Redacted]



T +32 [Redacted]
F +32 [Redacted]

M +32 [REDACTED]

E [REDACTED]

www.ge.com

*General Electric (GE)
2-4, Rond Point Schuman
1040 Brussels, Belgium*

[REDACTED]

From: [REDACTED]
Sent: 08 January 2016 11:44
To: [REDACTED]
Subject: FW: Request of meeting - [REDACTED] Google - 18/19 February 2016

Could open a case please?

From: [REDACTED]
Sent: [REDACTED]
To: BUTTARELLI Giovanni
Cc: [REDACTED]
Subject: Request of meeting - [REDACTED] Google - 18/19 February 2016

Caro Giovanni,

I trust this email finds you well.

I would like to inform you that [REDACTED], will be in Brussels on Thursday 18th and Friday 19th of February 2016, and if your agenda would allow it, it would be terrific if we could organize a meeting with you to discuss the developments on the debate around privacy and security in Europe.

Thank you in advance for your attention.

A presto.

[REDACTED]

--

This email may be confidential or privileged. If you received this communication by mistake, please don't forward it to anyone else, please erase all copies and attachments, and please let me know that it went to the wrong person. Thanks.

[REDACTED]

From: [REDACTED]@communitygroup.eu>
Sent: 22 January 2016 12:38
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Meeting request: [REDACTED], [REDACTED] Hewlett Packard Enterprise

Thank you very much, we look forward to the meeting. Mr [REDACTED] mobile number is + [REDACTED].

Best,
[REDACTED]

From: [REDACTED]
Sent: mardi 19 janvier 2016 10:25
To: [REDACTED]@communitygroup.eu>
Cc: [REDACTED]@communitygroup.eu>
Subject: RE: Meeting request: [REDACTED], [REDACTED] Hewlett Packard Enterprise

Dear Mr. [REDACTED]

Sorry for the late reply!

15:15 on 27th January is ok for Mr. Wiewiorowski. Here is Mr. Wiewiorowski's mobile phone number: +32 [REDACTED].

May I have Mr. [REDACTED] phone number as well in case there is a delay or something else.

Thanks in advance

Best regards



[REDACTED]
Administrative Assistant

☎ (+32) [REDACTED] | 📠 +32 [REDACTED] | 📧 MTS [REDACTED]

Email [REDACTED]

European Data Protection Supervisor

Postal address: Rue Wiertz 60, B-1047 Brussels

Office address: Rue Montoyer 30, B-1000 Brussels

🐦 @EU_EDPS | 🌐 www.edps.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

From: [REDACTED]@communitygroup.eu]
Sent: 12 January 2016 20:04
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Meeting request: [REDACTED], [REDACTED] Hewlett Packard Enterprise

Dear Ms [REDACTED],

I have checked with Mr [REDACTED] and he is able to meet on the 27th. Would immediately after Mr Wiewiorowski's speech, at 15.15, be a convenient time to meet.
If not, a meeting before his speech would also be possible.

Best,
[REDACTED]

From: [REDACTED]
Sent: mardi 12 janvier 2016 19:11
To: [REDACTED]
Cc: [REDACTED]@communitygroup.eu>
Subject: RE: Meeting request: [REDACTED], [REDACTED] Hewlett Packard Enterprise

Dear Ms [REDACTED],

Thanks for your quick response on this. In principle, that sounds fine as Mr [REDACTED] will also be attending the conference on the 27th.
I will get in touch with him to doublecheck his availability on the 27th and get back to you with a suggested time.

Best,
[REDACTED]

From: [REDACTED]
Sent: mardi 12 janvier 2016 15:02
To: [REDACTED]@communitygroup.eu>
Cc: [REDACTED]@communitygroup.eu>
Subject: RE: Meeting request: [REDACTED], [REDACTED] Hewlett Packard Enterprise

Dear Mr. [REDACTED],

Unfortunately Mr. Wiewiorowski will be on mission on 25 and 26 January 2016 but he will be happy to meet you in the frame of the CPDP conference.
You can both meet there if this ok for you. Mr. Wiewiorowski will be speaking on 27th at 2pm.

Thanks in advance

Best regards



Administrative Assistant
☎ (+32) [REDACTED] | 📠 +32 [REDACTED] | 📧 MTS [REDACTED]
Email [REDACTED]
European Data Protection Supervisor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels
🐦 @EU_EDPS 🌐 www.edps.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

From: [REDACTED]@communitygroup.eu]
Sent: 12 January 2016 14:28
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Meeting request: [REDACTED], [REDACTED] Hewlett Packard Enterprise

Dear Ms [REDACTED],

You may remember that back in November we were in contact regarding a potential meeting between Mr Wiewiorowski and Mr [REDACTED], [REDACTED] at Hewlett Packard Enterprise. In the end, we were not able to follow up on this, as Mr [REDACTED] cancelled his trip given the security situation in Brussels at the time.

Mr [REDACTED] has now rearranged his trip to Brussels and will be here on 25 and 26 January. He would very much like to arrange a meeting with Mr Wiewiorowski in order to discuss the ongoing safe harbour negotiations as well as the implementation of the General Data Protection Regulation.

Mr Pradelles availabilities for a meeting are:

- 26 Jan – all day, except between 15.00 and 16.30 (it is his preference to have a meeting on the 26th if possible)
- 25 Jan – afternoon

Would Mr Wiewiorowski be available for a meeting on either of these days? Looking forward to hearing from you.

Best wishes,

[REDACTED]

[REDACTED]

Community Public Affairs

6 Place Poelaert - 1000 Brussels – Belgium

Office: +32 [REDACTED]

Mob: +32 [REDACTED]
Mail to: [REDACTED]@communitygroup.eu
Learn more: www.communitypublicaffairs.eu

From: [REDACTED]
Sent: mercredi 25 novembre 2015 15:07
To: [REDACTED]@communitygroup.eu>
Cc: [REDACTED]@communitygroup.eu>
Subject: RE: Meeting request: [REDACTED], [REDACTED] Hewlett Packard Enterprise

Dear Mr [REDACTED]

Thank you for your e-mail!

Best regards



[REDACTED]
Administrative Assistant

☎ (+32) [REDACTED] | ☎ +32 [REDACTED] | ✉ MTS [REDACTED]

Email [REDACTED]

European Data Protection Supervisor

Postal address: Rue Wiertz 60, B-1047 Brussels

Office address: Rue Montoyer 30, B-1000 Brussels

🐦 @EU_EDPS 🌐 www.edps.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

From: [REDACTED]@communitygroup.eu]
Sent:
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Meeting request: [REDACTED], [REDACTED] Hewlett Packard Enterprise

Dear Ms [REDACTED],

I am afraid that with the IAPP being cancelled and the current situation in Brussels, Mr [REDACTED] is no longer coming to Brussels on those dates and will have to cancel the meeting. We would still very much like to organise a meeting with Mr Mr. Wiewiorowski in the future and will be back in touch when we have an idea when Mr [REDACTED] will next be in Brussels. We hope we can arrange something then. Sorry for any inconvenience.

Best wishes,

[REDACTED]

From: [REDACTED]
Sent: mardi 24 novembre 2015 12:46
To: [REDACTED]
Subject: RE: Meeting request: [REDACTED], [REDACTED] Hewlett Packard Enterprise

Dear Mr [REDACTED]

The IAPP conference being cancelled, would Mr. [REDACTED] still want to see Mr. Wiewiorowski at our premises or the meeting is cancelled too?

Thanks in advance

Best regards



[REDACTED]
Administrative Assistant
☎ (+32) [REDACTED] | ☎ +32 [REDACTED] | 📠 MTS [REDACTED]
Email [REDACTED]
European Data Protection Supervisor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels
🐦 @EU_EDPS 🌐 www.edps.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

From: [REDACTED] [communitygroup.eu](mailto:[REDACTED]@communitygroup.eu)
Sent: [REDACTED]
To: [REDACTED]
Subject: RE: Meeting request: [REDACTED], [REDACTED] Hewlett Packard Enterprise

Dear Ms [REDACTED],

I can now confirm that the most convenient time for Mr [REDACTED] would actually be **3pm on the 2nd December** (sorry to send contradictory emails) at the Square meeting centre.

Attending will be Mr [REDACTED] ([REDACTED], HPE) and a colleague of mine, Mr [REDACTED] ([REDACTED], Community Public Affairs).

Would you be able to share the contact phone number for Mr Wiewiorowski so that we can be sure to meet him without any complications.

Best,

From: [REDACTED]
Sent: lundi 16 novembre 2015 12:54
To: [REDACTED]
Subject: RE: Meeting request: [REDACTED], [REDACTED] Hewlett Packard Enterprise

Dear Ms [REDACTED],

Thanks for your follow up. The slot on the 1st December at 11:30 on the EDPS premises is likely to be the most convenient for Mr [REDACTED]. However, I am just waiting on confirmation on whether one of his colleagues (Ms [REDACTED]) is also able to join the meeting. I will get back to you with a final confirmation as soon as possible.

Best,

From: [REDACTED]
Sent: mercredi 11 novembre 2015 14:50
To: [REDACTED]@communitygroup.eu>
Subject: RE: Meeting request: [REDACTED], [REDACTED] Hewlett Packard Enterprise

Dear Mr [REDACTED]

Mr. Wiewiorowski would be pleased to meet Mr. [REDACTED] either in the premises of EDPS on 1st December at 11:30 either in the Square Conference on 2nd December at 3 pm before his panel starting at 4:30.
It might be easier for Mr. [REDACTED] to meet Mr. Wiewiorowski at the venue of IAPP Congress.

Could you please let me know what suits Mr. [REDACTED] best?

Thanks in advance

Best regards



[REDACTED]
Administrative Assistant

☎ (+32) [REDACTED] | 📠 +3 [REDACTED] | 📧 MTS [REDACTED]

Email [REDACTED]

European Data Protection Supervisor

Postal address: Rue Wiertz 60, B-1047 Brussels

Office address: Rue Montoyer 30, B-1000 Brussels

🐦 @EU_EDPS 🌐 www.edps.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure.

they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

Od: [REDACTED]@communitygroup.eu]
Wysłano: 10 listopada 2015 12:13
Do: WIEWIOROWSKI Wojciech
DW: [REDACTED]; [REDACTED]
Temat: Meeting request: [REDACTED], [REDACTED] Hewlett Packard Enterprise

Dear Mr Wiewiorowski,

I am writing on behalf of our client, Hewlett Packard Enterprise (HPE) to request a meeting between you and HPE's [REDACTED], [REDACTED]. We would like to take this opportunity to discuss with you the ongoing negotiations on the Safe Harbour decision as well as the adoption of the new Regulation on Data Protection. HPE has been supportive of the current reform of privacy rules in Europe as a necessary regulatory condition to the Digital Single Market. Like the EDPS, HPE sees trust as a competitive advantage for companies and has been a huge proponent of accountability and privacy by design as a way to restore confidence to data processing activities. However, recent developments with an impact on transatlantic transfers have blurred our perception of the EU's future digital ecosystem.

[REDACTED], who has recently assumed a new role as [REDACTED] following Hewlett Packard's split, will be in Brussels for the IAPP Congress in December. We would like to propose a meeting on the 1st of December anytime as of 10:30am, the 2nd from 2:30pm to 4:30pm or the 3rd anytime between 10:45 and lunch time. Please, let us know when it would be the most convenient for you to meet us.

Best regards,

[REDACTED]

[REDACTED]

Community Public Affairs

6 Place Poelaert - 1000 Brussels – Belgium

Office: +32 [REDACTED]

Mob: +32 [REDACTED]

Mail to: [REDACTED]@communitygroup.eu

Learn more: www.communitypublicaffairs.eu

[REDACTED]

From: HUSTINX Peter
Sent: 27 February 2013 16:10
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Meeting with Apple's Privacy Team

Dear Mr [REDACTED],

The meeting will be in our new office at Rue Montoyer 30 in Brussels
<http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Contact;jsessionid=C681E4D90C083C2E15CB0685DD12E540>

One or two staff members from relevant policy sectors might be joining in.

Kind regards,

Peter Hustinx



Peter Hustinx
Supervisor

Tel. +32 2 283 19 01 | Fax +32 2 283 19 50

 edps@edps.europa.eu

European Data Protection Supervisor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels

 [@EU_EDPS](https://twitter.com/EU_EDPS)  www.edps.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

From: [REDACTED]@apple.com]
Sent: 27 February 2013 16:02
To: HUSTINX Peter
Cc: [REDACTED]
Subject: Re: Meeting with Apple's Privacy Team

Dear Mr Hustinx

Could you please let me know where the meeting will take place, and who might join you in the meeting?

Kind regards

[REDACTED]

On 25 Feb 2013, at 12:01, HUSTINX Peter <peter.hustinx@edps.europa.eu> wrote:

Excellent and now blocked

From: [REDACTED]@apple.com]
Sent: 25 February 2013 11:44
To: HUSTINX Peter
Cc: [REDACTED]
Subject: Re: Meeting with Apple's Privacy Team

Dear Mr Hustinx

Thank you for your kind reply. Would it be possible to meet at 11:15 on 8 March?

Yours sincerely

[REDACTED]
[REDACTED]

Apple ▪
Square de Meeus, 37
B-1000 Brussels
Belgium

iPhone +32 [REDACTED]
Office +32 [REDACTED]
Fax +32 [REDACTED]
Email
[REDACTED]@apple.com

On 25 Feb 2013, at 11:23, HUSTINX Peter <peter.hustinx@edps.europa.eu> wrote:

Dear [REDACTED]

[REDACTED] would be most welcome for a meeting of about 45 y 8 March between 9.00 and 12.00.

Please let me know what would fit best in her schedule.

Kind regards,

Peter Hustinx



Peter Hustinx
Supervisor

Tel. +32 2 283 19 01 | Fax +32 2 283 19 50

 edps@edps.europa.eu

European Data Protection Supervisor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels

 [@EU_EDPS](https://twitter.com/EU_EDPS)  www.edps.europa.eu

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

From: [REDACTED] [apple.com](mailto:[REDACTED]@apple.com)
Sent: 21 February 2013 10:04
To: European Data Protection Supervisor
Subject: Meeting with Apple's Privacy Team

Dear Mr Hustinx

[REDACTED] Apple's [REDACTED], will be in Brussels on 7/8 March, and would like to meet with you to discuss developments in data protection, both for Apple and at the EU policy level. We would also like to take the opportunity to introduce [REDACTED], our new colleague in charge of [REDACTED].

I very much hope that you are available for a meeting, and look forward to hearing from you soon.

Yours sincerely

[REDACTED]
[REDACTED]

Apple •
Square de Meeus, 37
B-1000 Brussels
Belgium

iPhone +32 [REDACTED]
Office
+32 [REDACTED]
Fax +32 [REDACTED]
Email [REDACTED] [apple.com](mailto:[REDACTED]@apple.com)

<edps_logo.png><edps_web.png><edps_twitter.png><edps_m
ail.png>