# THE FUTURE OF PRIVACY

A report from a workshop co-organised by the Internet Society (Christine Runnegar) and the Electronic Frontier Foundation (Katitza Rodriguez) at the UN Internet Governance Forum (IGF) on 14 September 2010 at Vilnius, Lithuania.

## *INTRODUCTION*

Considerable efforts are being undertaken this year in various forums to assess whether existing privacy principles remain relevant and effective. 2010 and 2011 represent important milestones for privacy: 2010 marks the 30th anniversary of the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – the first step towards an international expression of agreed privacy principles. Preparations are also underway for the 30th anniversary of the Council of Europe Convention 108 – the first legally binding international privacy instrument – that will be held in January 2011. Additionally, last year (2009), the International Conference of Data Protection and Privacy Commissioners approved a non-binding resolution of new international privacy standards as "the basis for the drawing up of a future universally binding agreement ("the Madrid resolution").

All regions are taking a fresh look at Privacy, inviting stakeholders to express their views on existing laws and help identify the challenges and opportunities that lie ahead. For example, last year, the European Commission held a public consultation on the European legal framework for the fundamental right to protection of personal data. The U.S. Federal Trade Commission in late 2009-2010 held a series of public Privacy Roundtables "to explore the privacy challenges posed by the vast array of 21st century technology and business practices that collect and use consumer data". The Canadian Office of the Privacy Commissioner is also hosting a series of Consumer Privacy consultations this year "to promote debate about the impact of these technological developments on privacy, and to inform the next review process" for the Canadian PIPEDA Act.

As governments around the world are currently reviewing their privacy frameworks, we saw this workshop as an opportunity to take a step into the next decade and critically examine the future of privacy in the online environment.

### *The organisers*

The Internet Society (ISOC) is a non-profit organisation founded in 1992 to provide leadership in Internet related standards, education, and policy. With offices near Washington D.C., USA, and in Geneva, Switzerland, it is dedicated to ensuring the open development, evolution and use of the Internet for the benefit of people throughout the world. www.isoc.org

The Electronic Frontier Foundation (EFF) is an international civil society non-governmental organization with more than 14,000 members in 57 countries, which is dedicated to the protection of citizens' civil rights, and the creation of balanced copyright laws that enable access to knowledge and foster technology innovation. EFF works to ensure that the government complies with appropriate legal standards when it wants to conduct electronic surveillance or otherwise obtain users' data from third party communications service providers. www.eff.org

### *The panellists*

- Christine Runnegar, Senior Manager Public Policy, Internet Society
- Hugh Stevenson, Deputy Director for International Consumer Protection, Office of International Affairs, US Federal Trade Commission
- Rafael García Gozalo, Head of the International Department, Agencia Española de Protección de Datos, Spain
- Catherine Pozzo di Borgo, Council of Europe Consultative Committee of Convention 108 (T-PD)
- Joseph Alhadeff, Vice President for Global Public Policy and Chief Privacy Officer for Oracle Corporation
- Rosa Barcelo, Legal Adviser, European Data Protection Supervisor
- Ellen Blackler, Executive Director, Regulatory Planning & Policy, AT&T
- Kevin Bankston, Senior Staff Attorney, Electronic Frontier Foundation
- Pedro Less Andrade, Senior Policy Counsel Latin America, Google Inc

### *The moderators*

Katitza Rodriguez, International Rights Director, Electronic Frontier Foundation
Christine Runnegar, Senior Manager Public Policy, Internet Society
Cristos Velasco, Internet Society IGF Ambassador (remote moderator)

The moderators were assisted by some of the Internet Society's 2010 IGF Ambassadors[1], many of whom also actively contributed to the discussion.

### *The participants*

The workshop was very well attended with over 100 participants in the room plus remote participation.

[1] The IGF Ambassadors Programme is part of the Internet Society's *Next Generation Leaders Programme* (see http://www.isoc.org/leaders)

## *PERSPECTIVES FROM THE WORKSHOP*

### Insights from the Internet technical community

(presented by Ms. Runnegar, Internet Society)

Extensive work is being undertaken across the Internet technical community in privacy, data protection, identity management, provenance and other related fields. Much of this work is focused on improving technological privacy protections and developing tools that will allow Internet users to have greater control as to how they share personal data via the Internet. It is important that this work and the perspectives of the Internet technical community are taken into account in policy discussions regarding appropriate privacy frameworks for the future digital environment.

The Internet Society opened the workshop with a presentation of a collection of brief insights into the future of privacy provided by members of the Internet technical community:

- Internet Society (ISOC)
- Jon Peterson, Hannes Tschofenig and Bernard Aboba, Internet Architecture Board (IAB)
- Rigo Wenning and Thomas Roessler, World Wide Web Consortium (W3C)
- Kantara Initiative Privacy & Public Policy Work Group (P3WG)
- Gershon Janssen, Organization for the Advancement of Structured Information Standards (OASIS)
- Dr. Jose Manuel Gómez-Pérez, R&D Director, Intelligent Software Components (iSOCO) S.A.
- James Clarke, Program Manager / Project coordinator of INCO-TRUST, Waterford Institute of Technology, Future Internet Assembly 'caretaker'
- Antonio F. Gómez Skarmeta, University of Murcia Spain UMU (RTSI ISG INS Partner) Identity and Access Management for Networks and Services (ETSI INS) ETSI Industry Specification Group (ISG)
- Antonio F. Gómez Skarmeta, Researcher, University of Murcia Spain UMU
- Sam Coppens, Researcher and Ph.D. candidate in computer science and engineering at Multimedia Lab of Ghent
- John Morris, Cynthia Wong, Alissa Cooper, Center for Democracy & Technology (CDT).

Their insights regarding the future of privacy appear in annexure A to this report, however, we set out a selection here:

Please note, these are not necessarily consensus views –

- In the future, privacy will be redefined in response to changing social, technical, and regulatory realities. While the concept of privacy will remain contextual, individuals will become more actively engaged with the protection of their privacy by actively managing their identity and related personal data.

- The W3C, the IETF and the Internet community of privacy experts must work together to provide an online experience that conforms with user expectations of privacy and the emerging regulatory environment.

- To keep up with the speed of innovation at the application layer, the IETF needs to develop privacy guidelines, building blocks and tools that are useful for an entire class of applications.

- As a universal, distributed application platform, the Web links personal data across individuals, organizations, and countries. New sensor APIs also give Web applications access to users' location and to their physical environment.

- Technology helps users defend against some intrusions, and it helps users understand who learns what about them. But when the data about preferences and habits that fuels the business models behind today's ecosystem of free services is gleaned from users' online interactions, the policy framework needs to encourage privacy friendly behavior.

- The Kantara Initiative Privacy & Public Policy Work Group believes that it is important to support the open development of globally-applicable privacy standards, both technical and regulatory, in order to continue having confidence in the Internet ecosystem.

- Only by multi-stakeholder collaboration will viable solutions emerge, be deployed, and maintained.

- An effective solution would be a collection of privacy and security policy-configurable, IT-based, systematic behaviors that satisfy the requirements of privacy and security policies within a wide variety of contexts and implementation use-case scenarios.

### Hugh Stevenson, Deputy Director for International Consumer Protection, Office of International Affairs, US Federal Trade Commission

Mr. Stevenson (FTC) started by explaining the role of the U.S. Federal Trade Commission (FTC) vis-à-vis privacy and data protection in the United States. He provided a useful regulatory introduction to the workshop's consideration of the future of privacy by revisiting the past and moving through the present to the future.

Mr. Stevenson reported that the FTC is preparing a report from the results of the series of Privacy Roundtables held by the Commission in late 2009 – early 2010 "to explore the privacy challenges posed by the vast array of 21st century technology and business practices that collection and use consumer data". Some of the ideas coming from that series of roundtables include:

- Encourage business to integrate privacy and security at the outset
- Simplify consumer choice and recognise that more information is not necessarily helpful in helping the consumer handle his/her information

- Reduce consumer confusion and increase consumer understanding as to how their personal data will be handled

He suggested that it might be useful to consider how to simplify the choices consumers have to make with respect to their personal data.

In relation to international cooperation, Mr. Stevenson commented that this is very much a long-term process as privacy is issue about which there is sometimes narrow consensus. He added that the FTC believes in working to promote and establish networks to focus on collaboration in privacy enforcement.

Mr. Stevenson concluded by stating that the FTC welcomes comments on the privacy report when it is released.

### Rafael García Gozalo, Head of the International Department, Agencia Española de Protección de Datos, Spain

Mr. García Gozalo (Spanish Data Protection Agency), approaching the future of privacy from the perspective of a data protection authority emphasised that:

- The main concern for data protection is that existing regulations are difficult to implement to the Internet and Internet-based services – perhaps because they are territorial.

- We need to review laws with the aim of better adapting them to the characteristics of the Internet. Such reviews are already underway in the Europe, the U.S. and elsewhere. However, it is not enough to review laws, they need to be reviewed in a harmonious manner.

- The last conference of the International Data Protection and Privacy Commissioners adopted a resolution for international privacy standards (the Madrid Resolution) and is a step towards creating binding international principles.

- Reviewing laws is not the only solution – there also needs to be improved cooperation among data protection authorities. (In this regard, an initiative was launched recently to facilitate better cooperation among data protection authorities.)

### Catherine Pozzo di Borgo, Council of Europe Consultative Committee of Convention 108 (T-PD)

Mrs. di Borgo represented the Consultative Committee of Convention 108 (T-PD), the Council of Europe committee concerned with the protection of personal data in Europe. She provided an outline of the work being undertaken by the committee and explained why an expert appraisal of the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108)* has become necessary.

In examining the future of the Convention, Mrs. di Borgo observed, among other things:

- *Aim of the Convention*: "Today we might wonder whether the aim of the Convention, rather than being purely punitive (imposing strict data confidentiality and prohibiting certain types of processing), might not reflect a more positive approach by entitling the individual to control the use of his or her personal data?"

- *Concepts*: "Some concepts used in the 1981 text may have lost their relevance in the light of technological developments: the identifiable or "distinct" nature of the person, the concept of a file which might be enlarged to the broader concept of processing, etc."

- *Revising and creating new principles*: "The T-PD Bureau might also consider the need to encourage the development of and recourse to "privacy by design" technologies. This would seem necessary in order to restore confidence in the use of the new technologies and provide individuals with improved data protection systems. Privacy by design might be taken as a basic principle in this field."

- *Data Security*: "… in order to remedy network insecurity, we might consider laying down a requirement on enlarged security geared to not only preventing unauthorised access but also giving the data subjects control over access to their data.

  "This approach might be accompanied by a new obligation on those responsible for data processing to ensure that the data subjects are promptly informed if their personal data are wrongfully disclosed or used in a manner incompatible with the purpose for which they were gathered."

- *New rights and guarantees*: "Given the lack of transparency in network operations, new rights should be considered for data subjects to enable them to control their own data and also to guarantee a right to erasure of data."

On the issue of "consent", Ms. Pozzo di Borgo said:

> "We might note that Convention 108 does not assign any official status to the data subject's consent, whereas a number of services running on the Web do systematically ask for the person's consent in order to legitimate the relevant data processing operations. Nevertheless, consent may not appear to be a sufficient basis for legitimacy unless it is specific, informed and obtained by fair means, so it is fair to write it down as a principle in the Convention."

She concluded by stating:

> "With Convention 108 the Council of Europe has an instrument which has been genuinely effective for 30 years but which it would now like to analyse in order to guarantee its continuing efficiency and stability, in line with future technological developments."

## Joseph Alhadeff, Vice President for Global Public Policy and Chief Privacy Officer for Oracle Corporation

Joseph Alhadeff (Oracle Corporation) provided a merged enterprise-technology perspective to the future of privacy. In summary, Mr. Alhadeff emphasised:

- Global information flows, Web 3.0 and other innovations require new privacy paradigms.

- A paradigm of "accountability" is one such approach. Under this paradigm, the obligation to protect data flows with information. Accountability may be achieved with tools, practices, contracts, etc. and not just by relying on local law.

- For an accountability approach to be successful, it will need to have an effective, outcomes based framework that enables more simplified, flexible and less bureaucratic processes (registration, transfer) in return for a heightened demonstration of accountability by organisations.

- The concept of how to measure and validate accountability is only developing now and requires additional work.

- Privacy by design is one of the ways to demonstrate accountability. Privacy needs to be considered in the development of the process, not just at the points of its technical implementation.

- Control of personal data must be considered in the light of effectiveness and usability. Granularity of control needs to enhance choice not create confusion or burden.

- Global, divergent approaches to privacy need to be interoperable.

## Rosa Barcelo, Legal Adviser, European Data Protection Supervisor

Mrs. Barcelo (EDPA) gave the perspective of the European Data Protection Supervisor "… an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies".[2]

She made six keys points:

- We are pleased to see the *European Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (95/46/EC) under review. Some changes are needed to adapt the directive to new technologies. At the end of 2010, the European Commission will adopt a communication that will put forward the main changes for the possible review of the Data Protection Directive. Then mid 2011, the Commission will submit a proposal to the Parliament.

[2] http://www.edps.europa.eu/EDPSWEB/edps/EDPS?lang=en

- The review of the directive should not "water-down" existing rights, the right to access to one's personal information, transparency, they should remain and should not be refused. However, we might see some changes in these existing rights to adapt them to the online environment (e.g. traditionally, access rights have been given in paper, and this might be changed slightly to emphasise the online world).

- New rights might be added. For example: a right to be left alone; a right to accountability (Note: The right of accountability would require data controllers to comply not only with the data protection principles but to put in place organisational measures to demonstrate compliance); a right to privacy-by-design. (Note: privacy-by-design would require not only the data protection principles embedded in the technology, but also embedded within the whole organisation, from the beginning to the end of the process.)

- We support notification of data security breaches to all data controllers.

- There is insufficient police cooperation – a police/justice vacuum in the area of data protection needs to be covered.

- There needs to be a comprehensive framework.

Mrs. Barcelo also said they would like to see the possibility of collective action for privacy breaches (e.g. the possibility for consumer associations and others to bring an action on behalf of multiple consumers).

### Ellen Blackler, Executive Director, Regulatory Planning & Policy, AT&T

Mrs. Blackler (AT&T) focused on consumer usability and emphasised that the business industry needs to innovate around usability.

On the topic of user control of data, Mrs. Blacker commented that control needs to be usable and observed that sometimes the level of granularity of control offered to consumers can be overwhelming. She provided some suggestions, including:

- Interoperable permissions – so consumers do not have to state their privacy preferences for each individual transaction

- Feature-ised privacy – so that it is easier for consumers to understand what information is collection and used with each feature.

Mrs. Blackler stressed that this about making a paradigm shift – not building walls. We need to find a way to allow consumers to share information with their control which is very different from wanting to lock up their data.

### Kevin Bankston, Senior Staff Attorney, Electronic Frontier Foundation

Kevin Bankston (EFF) spoke primarily about The Future of Privacy vis-à-vis the government, and especially about government access to citizens' private communications and related communications records.

Mr. Bankston said that too much of communications privacy law, both in the US and elsewhere, is still premised on three outdated and increasingly false dichotomies:

- **(1) The dichotomy between data stored by a user and data stored for a user by a provider.** Privacy law has typically provided strong protections against government intrusion into information that you store personally (e.g. on your home computer or in your office files), while providing much less protection for data you store with a third party provider. In an age where countless millions are trusting web-based email services such as Microsoft's Hotmail to store years worth of private correspondence and cloud services such as Google's Docs to store their most private documents, it is time for privacy law to treat such online storage as an extension of your own home or office.
- **(2) The dichotomy between prospective and retrospective communications surveillance.** Privacy law, for example, in the United States provides very strong protections against government surveillance of your communications as they happen—prospective or "real-time" wiretapping or monitoring of your phone or internet traffic—while providing much weaker protections against government intrusion into previously-stored communications. For example, in the U.S., if the government wants to wiretap your email, it must first obtain a judge-issued search warrant, showing probable cause that a crime has been or is being committed—a very high standard—and must also follow a variety of other strict privacy-protective procedures. In contrast, when it comes to previously-stored emails, the U.S. Department of Justice's practice is to obtain every message in an email account with only a subpoena issued by an individual prosecutor, based on that prosecutor's individual judgment and without any court oversight or approval. This is true despite the fact that accessing years and years worth of your private stored emails is in many cases likely to be much more invasive than a thirty-day wiretap on your email.

- **(3) The dichotomy between the content of a communication and non-content information about that communication.** The contents of communications are typically strongly protected by privacy law whereas non-content transactional data or "meta-data" is typically much less protected, even though it can be just as revealing. A dossier of everyone you communicate with by email, instant message, and VOIP, when you communicate and how much data you communicate, can be intensely revealing; for example, researchers at MIT demonstrated this fact when they were able to accurately predict a person's sexual orientation based on who their Facebook friends were, and one can easily imagine how such data could be equally revealing of other political, religious, and economic associations. Meanwhile, monitoring of other data that is arguably transactional and not content—the location of your cell phone, clickstream data revealing the web sites you visit and search logs indicating what you searched for using Google or another search engine—is just as invasive as reading your email or listening to your phone calls.

Mr. Bankston concluded that we must move past these outdated dichotomies, which new technology is quickly rendering useless. He said we should focus on the invasiveness of the surveillance techniques at issue rather than focusing on where the data is stored,

whether the surveillance is retrospective or prospective, or whether the data is content or not.

A copy of Mr. Bankston's speaking notes appears in annexure C.

### Pedro Less Andrade, Senior Policy Counsel Latin America, Google Inc

Pedro Less (Google Inc.) completed the panel presentations focusing on the role of Internet intermediaries, specifically Web search engine providers. In summary, Mr. Less said:

- Privacy principles should be revised in light of new technologies.
- Search engines are neutral technologies and should remain neutral.
- Search engines and freedom go, or should go, hand-in-hand, as long as search engines do not assume control of the information. Where search engines start to assume control of information, there is a danger to democracy and freedom.
- Search engines should be instruments of freedom, accurate and accessible democratic knowledge. In order to assure this, it is important to include Intermediary Liability Exceptions for intermediary services providers in new revised privacy principles.
- Where the user exercises discretion as to how information is stored, processed or referenced, that user should be considered "the data controller" – i.e. someone who is competent to decide about the contents and use of personal data (regardless of whether or not such data is collected, stored, processed or disseminated him or her, by an agent or by intermediary service provider on his or her behalf) and not the service provider who has no actual knowledge that the material, or an activity using the material, on its system or network infringes someone's privacy.
- Actions against Internet intermediaries, which operate neutral technologies and do not have control over third party content, based on the protection of privacy could constitute ways of indirect censorship and could have a chilling effect over speech. For that reason, such actions should be addressed against the creators of the content that infringe people's privacy.

### *DISCUSSION*

The participant discussion helped to elaborate the panel presentations and inject further new ideas into the dialogue. Some examples are set out below.

In the context of discussing individual consent and control over personal data, Mr. Stevenson commented that one of challenges is to convey information in a meaningful way, particularly where privacy statements/policies are very long and detailed. He emphasised that the key point is "understanding", i.e. what information does an individual need to make a meaningful decision so as to have more control over his/her

data. Further, Mr. Alhadeff noted that the level of granularity of control offered can also be overwhelming, observing that some individuals may be capable of exercising this level of control, but others may not. He reiterated the point made by Mrs. Blackler that usability is essential. Mr. Less added that Google Inc., recognising this issue, has recently made some important changes to its privacy policies to make them simpler for Google product users to understand. He also suggested that privacy needs to be seen by business as a competitive advantage.

As to privacy laws internationally, there appeared to be general consensus that there is value in moving, to the extent practicable, towards a consistent approach across jurisdictions. However, approaches to achieving this goal may vary. Mr. García Gozalo had proposed the term "harmonization" earlier, and Mr. Stevenson, noting various difficulties with achieving complete uniformity between different legal systems, used the term "convergence". Ms. Pozzo di Borgo added that the Council of Europe would like to make Convention 108 available for signature by countries outside Europe.

Mr. Velasco observed that the Madrid resolution has been a very useful guide for developing countries that do not have active data protection laws, but it needs specific provisions regarding cross-border jurisdiction and conflicts of laws.

Ms. Grace Bomu from Kenya, one of the Internet Society Ambassadors, speaking in her personal capacity, asked the panel whether there is consensus (e.g. in Europe or North America) on whether there should be a right to be forgotten. One of the panellists responded that privacy experts are considering this issue, but that more discussion needs to take place: it may be a good thing or it may not.

A remote participant raised a question regarding the applicability of data protection laws to RFID technologies. Mr. Alhadeff responded that there is no reason in principle why they should not apply, but that their application may have to be different (e.g. there may not be space on the device for a notice, so perhaps small symbols may be required). While Ms. Pozzo di Borgo agreed in principle, she commented that because RFID is new, care needs to be taken regarding the application of data protection principles.

## ***CONCLUSIONS***

It is important to emphasise in this report that considerable efforts are already being undertaken in many forums across the world to assess whether existing privacy principles remain relevant and effective in the 2010 and post 2010 environment. For example - the reviews of the:

- OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*
- *European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*
- *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*

as well as public consultations conducted by the United States Federal Trade Commission, the Canadian Office of the Privacy Commissioner and other governments. We look forward to the outcomes of these reviews and consultations.

The workshop was an information sharing exercise and as such participants did not attempt to reach any consensus conclusions. Nonetheless, we wish to list here some of the points that were made during the workshop as they prove useful in future policy discussions on privacy frameworks.

Please note that these points reflect some of the views of particular participants and are not necessarily consensus views. Further, in the time allocated, it was not always possible for participants to comment on all views that were expressed.

As these points are but a selection, we encourage the reader to read the whole report.

- In a world of global data flows and new technologies:
    - privacy laws need to be harmonized (or perhaps, rather there needs to be convergence) with the aim of better adapting those laws to the characteristics of the Internet;
    - international cooperation among data protection authorities needs to be improved; and
    - resources need to be allocated to enforcement.
- There are some challenges to achieving broad international harmonisation because privacy is a broad subject with limited international consensus in certain areas. Indeed, even at the domestic and regional level, privacy issues are currently undergoing re-examination. Further, there are also the significicant difficulties introduced by jurisdiction and conflicts of law.
- It is important to support the open development of globally-applicable privacy standards, both technical and regulatory, to continue having confidence in the Internet Ecosystem.
- Only by multi-stakeholder collaboration will viable solutions emerge, be deployed, and maintained.
- Data protection must take into account many different rights and dovetail with other laws geared to ensuring the protection of individuals.
- New paradigms will need to be considered – for example, accountability (i.e. the obligation to put in place appropriate and effective measures to protect personal data, independently of where the information flows).
- Privacy by design is a concept of people, processes, practices and technology – privacy principles need to be embedded in the design from the very beginning right through to the end.

- There needs to be innovation and focus on usability of solutions that offer individuals control over their personal data.

- Transparency in data collection and processing is important to equip consumers so they can make informed choices, and give informed consent to the collection, use and disclosure of their personal data.

- Consent should be informed, freely given and obtained through fair means.

- Further work needs to be undertaken to inform and educate people as to how their personal data is being collected and used.

- The future of privacy should include the protection of privacy vis-à-vis the governments, and especially legal safeguards against government access to citizens' private communications, and related communications records.

Finally, further information regarding the workshop conversations is available on the UN Internet Governance Forum website.[3]

***IGF MAIN SESSION – SECURITY, OPENNESS AND PRIVACY***

The Internet Society presented a very brief report on The Future of Privacy workshop during the IGF main session on Security, Openness and Privacy on 16 September 2010, summarising various views expressed by some of the participants regarding international cooperation on privacy. Details of this report appear in annexure D.

***THANK YOU***

The Electronic Frontier Foundation and the Internet Society would like to express our thanks to the IGF Secretariat, panellists, moderators, participants (in-room and remote) as well as the assisting Internet Society IGF ambassadors for making this a very successful workshop.

The Internet Society would also like to thank the Internet technical community for supporting the Internet Society in this endeavour and contributing very considered and insightful perspectives on the Future of Privacy (www.isoc.org/privacyinsights). This is part of an ongoing effort by the Internet Society to bring Internet technical expertise and perspectives to the policy debate on privacy.

***ONGOING WORK***

The Internet Society will continue collecting and documenting insights on the Future of Privacy from the Internet technical community for input into policy discussions on privacy. We invite you to send your contribution (max 100 words or a picture) to isoc@isoc.org.

[3] Transcript at http://www.intgovforum.org/cms/component/content/article/102-transcripts2010/636-66; Webcast at http://webcast.intgovforum.org/ondemand/?media=workshops

We also invite Internet Society members and others to express their views on The Future of Privacy here: http://isoc.org/wp/privacy.

***MEDIA COVERAGE***

Larry Magid, *Internet Governance Forum Tackles Online Privacy*, Huffingtonpost, (September 15, 2010), available at http://www.huffingtonpost.com/larry-magid/internet-governance-forum_b_717392.html.

## Annexure A

### INSIGHTS FROM THE INTERNET TECHNICAL COMMUNITY

### The Internet Society (ISOC)

- In the future, privacy will be redefined in response to changing social, technical, and regulatory realities. While the concept of privacy will remain contextual, individuals will become more actively engaged with the protection of their privacy by actively managing their identity and related personal data.
- People will be more informed custodians of their personal data – able to help decide when the sharing of personal information requires explicit consent, and choosing appropriate levels of security and protection.
- Internet-based solutions to support user-managed privacy protection are emerging, and the Internet Society is helping to provide clarity about their use to individuals, enterprise, and governments.

### Jon Peterson, Hannes Tschofenig and Bernard Aboba, Internet Architecture Board (IAB)

- The W3C, the IETF and the Internet community of privacy experts must work together to provide an online experience that conforms with user expectations of privacy and the emerging regulatory environment.
- To keep up with the speed of innovation at the application layer, the IETF needs to develop privacy guidelines, building blocks and tools that are useful for an entire class of applications.
- Technical work needs to be backed-up by providing incentives to incorporate privacy into system design and at the same time to keep the speed of innovation and the openness of the Internet intact.
- The best technology will not help end users if it does not get implemented properly and deployed in a privacy friendly way.[4]

### Rigo Wenning and Thomas Roessler, World Wide Web Consortium (W3C)

- As a universal, distributed application platform, the Web links personal data across individuals, organizations, and countries. New sensor APIs also give Web applications access to users' location and to their physical environment.
- Everyday events – from the morning run to the credit card payment – are automatically brought online and shared online among friends and strangers.

[4] http://www.isoc.org/pubpolpillar/docs/IAB_position-paper-privacy.pdf

- Technology helps users defend against some intrusions, and it helps users understand who learns what about them. But when the data about preferences and habits that fuels the business models behind today's ecosystem of free services is gleaned from users' online interactions, the policy framework needs to encourage privacy friendly behavior.

## The Kantara Initiative Privacy & Public Policy Work Group (P3WG)

- The Kantara Initiative Privacy & Public Policy Work Group (P3WG) believes that it is important to support the open development of globally-applicable privacy standards, both technical and regulatory, in order to continue having confidence in the Internet ecosystem.
- To do so, the P3WG actively engages with individuals, enterprises, policymakers, regulators and adoption communities on best practices and common solutions.
- Fundamental to effective privacy are transparent architectures that secure private information and enable information-sharing in a secure, privacy-enhancing manner.
- Only by multi-stakeholder collaboration will viable solutions emerge, be deployed, and maintained.

## OASIS (Organization for the Advancement of Structured Information Standards)

- The state of privacy and information protection has changed substantially because of changes in technology, business models, and the role of the individual, bringing ever significant challenges to effective application of traditional privacy management.
- Implementing policies for increasingly federated networks, systems and applications is a problem as typical policy expressions provide little insight into how to actually implement them, as well as the lack of standards-based technical privacy frameworks or reference models that can enable development and implementation of privacy and associated security requirements.
- An effective solution would be a collection of privacy and security policy-configurable, IT-based, systematic behaviors that satisfy the requirements of privacy and security policies within a wide variety of contexts and implementation use-case scenarios.

## Dr. Jose Manuel Gómez-Pérez, R&D Director, Intelligent Software Components (iSOCO) S.A.

- The Internet provides us with more and more online services, virtualized online for our own convenience, which relieve us from cumbersome installation and configuration processes. It is possible to write email, compose and share documents, virtually everything, without installing a piece of software in our computers beyond a web browser. However, as usual, such advantages also have a price to pay, in this case in terms of a potential privacy loss. For example, online email services usually scan and process our emails, sending us personalized

advertisements and offering other potentially interesting (but usually undesired) services.

- In general, the processes by which our own personal data are manipulated are often opaque to us, but citizens have the right to have knowledge of the logic involved in any process concerning their personal data (EU directive D 95/46).

- These rights can only be enforced by a combination of legal but also automated means that analyze the provenance of the data [1] to support users in understanding such processes, are capable to determine what and by whom has been done with the data (attribution), and determine whether the processes are compliant with established contracts (accountability), while facilitating the analysis of the (potentially large and complex) processes by the users themselves (abstraction).

  [1] http://www.w3.org/2005/Incubator/prov

**James Clarke, Programme Manager/Project Coordinator of INCO-TRUST, Waterford Institute of Technology, Future Internet Assembly "caretaker".**

- It is important to ensure that privacy is addressed as fundamental to the design and development of the 'Future Internet' as an aspect of maintaining the digital rights, dignity and sovereignty of the citizen.[5]

**Antonio F. Gómez Skarmeta, University of Murcia Spain UMU (RTSI ISG INS Partner), Identity and Access Management for Networks and Services (ETSI INS) ETSI Industry Specification Group (ISG)**

- Today, the need for Identity Management is present whenever the user needs to login or the provider needs information about the user.

- Information, authentication and authorization should be consistent and act as the glue between the different applications the user interacts with.

- This will be especially important in Network and Service Providers in relation to the user's control of his/her identity and privacy.

- In future Distributed Identity Management Platform the user should be able to deal with various services, specify the preferences regarding the information revealed, and especially within privacy policy enforcement with respect to usage of quest and with regards to the attribute provider's privacy policy and user policies on what to disclose.

[5] [James Clarke] - As a Future Internet Assembly "caretaker", I am involved in the organisation of a session dedicated to privacy and citizenship at the upcoming FIA Ghent workshop being held 16-17th December 2010. The session will address the relationships between the involved technologies and the relevant stakeholders (citizens) to ensure that privacy is addressed as fundamental to the design and development of the "Future Internet" as an aspect of maintaining the digital rights, dignity and sovereignty of the citizen. The session will address topics concerning user/citizen issues related to privacy and economics of privacy. The sessions will highlight the ongoing work in these areas and the future work that needs to be done in order to empower citizens to feel confident in their communications on the Future Internet and to exercise choice over how their own information is being used. If you are interested in participating or contributing to this session, please contact the author and visit the web sites http://security.future-internet.eu/index.php/FIA_Ghent and http://www.fi-gent.eu

### Antonio F. Gómez Skarmeta, Researcher, University of Murcia Spain UMU

- Future Identity Frameworks should provide privacy-enabled Future Internet using Identities such that user control is maximized at all layer.
- User in the center of the control of its data and where they are stored and who use/access it.
- More controlled privacy than today: Not letting technology dictate level of privacy (IP addresses in the network)
- The capability to establish zones of privacy as in real life
- Controlled linkability and identity disclosure for accountability
- Capability of "limited identities" for minors
- Identity, Privacy and Trust as a key enabler of a Citizen Living Use Case in Future Internet

### Sam Coppens, Researcher and Ph.D. candidate in computer science and engineering at Multimedia Lab of Ghent

- Nowadays, the Internet has become such a big information space, people need technologies to filter out the information of interest. Examples are recommendation engines, RSS, social networks, etc. This leads to a situation where the Web has become a giant storage space for profile information on which the technologies rely to target the user with the information of interest. This profile information gets exchanged, even traded on the Internet like any other piece of information. People have no control anymore over this profile. The problem gets worse, because all this information is stored on a medium that has no expiration date. What ends up on the Internet, stays on the Internet. E.g., you can delete a photo on a certain social network, but chances are big it is already cached by some search engine, making it very hard to delete every trace of that photo.
- So, the users must recover full control over their profile information and this information, actually information in general, on the Internet should get an expiration date.

### Center for Democracy and Technology (CDT)

The Future of Privacy and Global Information Flows[6]

- Substantive consumer protections facilitate global flows of information
  - Growing recognition that the opt-in vs. opt-out debate is insufficient.
  - Emphasis on the responsibilities of companies to comply with the full range of Fair Information Practice principles (FIPs).

[6] PDF slide - document

    - Likely implementation of accountability programs, consumer access and control tools, and other mechanisms to both protect consumer privacy and encourage innovation.

- Recognition of these principles within the US and US government:
    - US privacy bill is introduced and receives industry support.
    - US Department of Commerce initiative emphasizes that privacy protections and global commerce and innovation are intertwined.
- Privacy protections should facilitate, rather than impede, free speech, the creation of user-generated content, and the proliferation of innovative platforms and services.

## Annexure B


**Internet Governance Forum**
14-17 September 2010
Vilnius

**Future of Privacy**
Contribution by Ms Pozzo di Borgo[7]

Thank you for inviting me here today. I am delighted to be representing the Consultative Committee of Convention 108 (T-PD), which is the Council of Europe committee dealing with the protection of personal data.

I would like to preface my comments by pointing out that private life and data protection are subjects to which the Council of Europe attaches the utmost importance. These subjects are addressed by the Council of Europe's Consultative Committee of Convention 108, which I am representing here today.

This Committee comprises members of national bodies responsible for data protection.

Its work exclusively concerns the application of Convention 108. More specifically, in 2003 it adopted a preparatory report on the use of biometric technologies, the first European document on this subject. More recently, it has prepared a draft Recommendation on profiling.

Data protection and Convention 108 are currently at a crossroads. The Convention, like many other instruments, was drawn up at a time when Internet was in its infancy, mobile phones were few and far between and people communicated by post.

So, for instance, the recent debates on film and music downloads which infringe copyright and the questions raised by the use of such facilities as Facebook, Google, StreetView, RFID chips and global data transfers highlight the need for a review of the whole area of personal data protection.

Current technological developments are making it painfully clear that data protection is at a crossroads in many respects.

Such protection must, firstly, take account of many different rights, including the freedom of expression, the right to information and intellectual property rights.

Secondly, it must dovetail with the application of legal texts geared to ensuring the protection of individuals, particularly minors, for example on the Internet.

[7] Vice-Chair of the Consultative Committee of the Convention for the protection of individuals with regards to automatic processing of personal data

Thirdly and lastly, it must be compatible with increasing individual mobility, market globalisation and the opportunities provided by the new technologies for customised exchange services.

An expert appraisal of Convention 108 has therefore become necessary, following the example of the current work on Directive 95/46/EC and on specific pieces of national legislation, in order to ensure that this treaty is still relevant to the new technologies.

It is important that Convention 108 should retain its place at the European, and indeed international, level.

The Council of Europe's T-PD Committee has therefore decided to continue the discussions which have been going on since 2004 on the need to tailor Convention 108 to new technological developments.

With this in mind, the T-PD has mandated its Bureau to carry out a broad analysis of the principles of Convention 108 as quickly as possible, in the light of current technological developments and the demands of the industry and civil society.

In order to do so, and taking into consideration the numerous technological aspects involved, the T-PD will bring together the opinions of the various interlocutors.

**Possible avenues of inquiry**

There are several possible avenues of inquiry into the aforementioned developments. I will be mentioning them here only as examples, without any particular order of priority or importance. Nor should they prejudge in any way the future work in this field within the T-PD Bureau.

The discussions might concern the aim pursued by the Convention, or its scope, or the data protection principles and the guarantees set out by the Convention in 1981.

**Changing the aim of Convention 108?**

It is interesting to note that according to Article 1 of Convention 108, the requisite data protection for each individual involves "respect for his rights and fundamental freedoms and in particular his right to privacy, with regard to automatic processing of personal data relating to him".

Today we might wonder whether the aim of the Convention, rather than being purely punitive (imposing strict data confidentiality and prohibiting certain types of processing), might not reflect a more positive approach by entitling the individual to control the use of his or her personal data?

Is it necessary to clearly enshrine such a right at a time when technologies, more by configuration than by necessity, generate and store traces of the use of services, which facilitates more detailed knowledge of the person and his or her behaviour, without any supervision?

**Changing certain concepts?**

Some concepts used in the 1981 text may have lost their relevance in the light of technological developments: the identifiable or "distinct" nature of the person, the concept of a file which might be enlarged to the broader concept of processing, etc.

**Revising some of the data protection principles and providing for new ones?**

We might note that Convention 108 does not assign any official status to the data subject's consent, whereas a number of services running on the Web do systematically ask for the person's consent in order to legitimate the relevant data processing operations.

The T-PD Bureau might also consider the need to encourage the development of and recourse to "privacy by design" technologies. This would seem necessary in order to restore confidence in the use of the new technologies and provide individuals with improved data protection systems. Privacy by design might be taken as a basic principle in this field.

**Reconsidering the scope of the guarantees of Convention No. 108?**

Convention 108 adopts a restricted approach to security, confining it to destroying data and protecting confidentiality. But in order to remedy network insecurity, we might consider laying down a requirement on enlarged security geared to not only preventing unauthorised access but also giving the data subjects control over access to their data.

This approach might be accompanied by a new obligation on those responsible for data processing to ensure that the data subjects are promptly informed if their personal data are wrongfully disclosed or used in a manner incompatible with the purpose for which they were gathered.

**Laying down new rights and guarantees?**

Given the lack of transparency in network operations, new rights should be considered for data subjects to enable them to control their own data and also to guarantee a right to erasure of data.

The T-PD Bureau must analyse the need for such new rights: the right to object in the field of geolocation facilities, the right not to be stalked, the right of enlarged access, the right not to be bound by a decision taken by a machine, the right to have data deleted, etc.

Of all these rights, the right to oblivion should probably be more carefully analysed in the light of current debates on the subject at an international level. This idea that information should not be permanent is a genuine matter for concern which can be addressed technologically by computer programmes that facilitate selective erasure of data.

I have pointed out some avenues which will be explored by the T-PD Bureau and T-PD itself and would invite the representatives of other institutions, industry and civil society to participate in further reflexion.

In conclusion, as I have pointed out, with Convention 108 the Council of Europe has an instrument which has been genuinely effective for 30 years but which it would now like to analyse in order to guarantee its continuing efficiency and stability, in line with future technological developments.

## Annexure C

### IGF 2010 The Future of Privacy Workshop

Contribution of Kevin S. Bankston

Senior Staff Attorney

The Electronic Frontier Foundation

Thank you for inviting me to speak here today. I am very pleased this morning to share the perspective of the Electronic Frontier Foundation on the future of privacy, and to be attending my very first Internet Governance Forum meeting; I very much hope it will not be the last.

My primary perspective is that of a litigator of privacy issues under US law, where I work to ensure our government's compliance with appropriate legal standards when it conducts electronic surveillance or obtains user data from communications providers, and, when those standards are in dispute, to establish the most privacy protective standards possible.

So, for example, I am one of the lead attorneys in EFF's lawsuits against the US National Security Agency and AT&T over our government's warrantless wiretapping program, and often face off in court with our government to try and ensure that investigators obtain search warrants based on probable cause before they, for example, attempt to track the location of a suspect's cell phone or obtain private emails from a suspect's email provider.

Despite my admittedly provincial perspective, I humbly believe that I have identified a few key concepts concerning communications privacy that we must consider critically when we consider the future of privacy.

In particular, I believe that preserving the future of privacy when it comes to our telephone and Internet communications turns on our overcoming the past and moving away from the outdated assumptions and prejudices that have guided communications privacy law and policy in the 20th century.

Specifically, I ask you to consider three dichotomies that pervade American privacy law and the law of many other nations, and that have defined our dialogue on communications privacy rights over the past decades. EFF believes these three dichotomies have been rendered false and counter-productive as technology has advanced, and that we must move past these old ideas and toward new ways of thinking about communications and data privacy in the 21st century.

THE FIRST outdated privacy dichotomy is that between data that is stored in your own home or office, on your own computer or in your own filing cabinet, which privacy law has typically protected very strongly against government intrusion, and that data which you store with a third party service provider, which has been viewed as less deserving of privacy. In an age where countless millions are trusting web-based email services such

as Microsoft's Hotmail to store years worth of private correspondence and cloud services such as Google's Docs to store their most private documents, it is time for privacy law to treat such online storage as an extension of your own home or office.

THE SECOND increasingly false dichotomy is between government surveillance of your communications as they happen, which the law strongly protects against, and surveillance of your past communications, which the government is allowed to do under much more liberal standards.

For example, under American law, if the government wants to wiretap your email and monitor your communications in real time, it must obtain from a judge a search warrant based on a showing of probable cause that a crime has been or is being committed. Such wiretapping also is subject to additional protective requirements—the government may only conduct such surveillance after exhausting all other investigative methods, can only use such techniques to investigate the most serious crimes, and must work to minimize the acquisition of communications that are not relevant to its investigation.

In contrast, when it comes to obtaining past emails, our Justice Department's practice is to merely have a prosecutor issue a subpoena based on its own judgment that the email account will contain relevant information, without court oversight, without probable cause, without having exhausted other methods, and without minimizing its acquisition of irrelevant data.

Yet can we say now in 2010 that 30 days of real time monitoring of your email—the typical length of a court-authorized wiretap--is really so much more invasive than accessing years and years of past email correspondence from your Gmail or Yahoo mail account? EFF thinks not.

The third and final false dichotomy is that between the contents of communications, which are usually strongly protected by law, and non-content transactional data or meta-data, the privacy of which is typically much less protected. We at EFF question whether this distinction ever made sense, even in the telephone context. But today, on the Internet, the line between the two is increasingly blurry, and your so-called transactional data can often be as revealing if not more revealing than, for example a wiretap on your phone. A dossier of everyone you communicate with by email, IM, skype and telephone, when you communicate and how much data you communicate, can be intensely revealing—researchers at MIT demonstrated this fact when they were able to accurately predict a person's sexual orientation based on who their Facebook friends were, and one can easily imagine how such data could be equally revealing of political, religious, and economic associations. Meanwhile, monitoring of other data that is arguably transactional—the location of your cell phone, clickstream data revealing the web sites you visit and search logs indicating what you searched for using Google or another search engine—should, in our view, be considered just as invasive as reading your email or listening to your phone calls.

EFF believes we must move past these false dichotomies and re-examine the laws that control government surveillance of communications with new eyes, ignoring past distinctions that technology has rendered moot and focusing solely on the invasiveness of the surveillance techniques at issue.

In the US, EFF has worked to move past these old privacy models both in court, and, as part of the Digital Due Process coalition, in our Congress. That coalition is an unprecedented alliance of civil society groups such as EFF, the American Civil Liberties Union and the Center for Democracy and Technology, working in concert with private sector companies such as Google, Microsoft, AOL, Amazon.com, eBay, Facebook, and even our court-room opponent AT&T. Although we may have our disagreements, we all do agree that the electronic communications privacy law in the US, most of which was written nearly 25 years ago, is outdated and needs to be simplified, clarified, and unified to better protect privacy and innovation and increase consumer confidence in emerging cloud and location-based technologies.

Therefore, and in closing, my final hope for the future of privacy—beyond moving past the three dichotomies I spoke of--is that this Digital Due Process effort might provide a model for civil society and corporate cooperation in the realm of privacy in other nations.

Thank you for your time and I look forward to your questions.

## Annexure D

## REPORT TO THE MAIN SESSION ON SECURITY, OPENNESS AND PRIVACY

Christine Runnegar from the Internet Society. Reporting for Workshop 66 – The Future of Privacy.

I would like to thank the organisers of this session for the opportunity to provide input to this discussion, and to thank the panellists, in-room and remote participants of the workshop for their valuable perspectives on the future of privacy.

### Theme 3: International cooperation on security, privacy and openness

The following points reflect some of the views of particular participants on this theme and are not necessarily consensus views. In the time permitted, it is, of course, impossible to cover all of the points that were made.

- In a world of global data flows and new technologies, privacy laws need to be harmonized (or there needs to be convergence) with the aim of better adapting those laws to the characteristics of the Internet, international cooperation among data protection authorities needs to be improved, and resources need to be allocated to enforcement

- It is important to note the considerable efforts currently being undertaken in various forums to assess whether existing privacy principles remain relevant and effective. For example: the reviews of the OECD's Privacy Guidelines, the European Convention 108 and the European Data Protection Directive.

- Other examples include: The U.S. Federal Trade Commission series of public Privacy Roundtables and the Canadian Office of the Privacy Commissioner's series of Consumer Privacy consultations.

- There are challenges to achieving broad international harmonization because privacy is a broad subject matter with limited international consensus in certain areas, and indeed even at the domestic and regional level, privacy issues are currently undergoing re-examination; there are also the significant difficulties introduced by jurisdiction and conflicts of law.

- It is important to support the open development of globally-applicable privacy standards, both technical and regulatory, to continue having confidence in the Internet Ecosystem.

- Transparent architectures that secure private information and enable information-sharing in a secure, privacy-enhancing manner are fundamental to effective privacy.

- Technical work needs to be backed-up by providing incentives to incorporate privacy into system design and at the same time to keep the speed of innovation and the openness of the Internet intact.

- Data protection must take into account many different rights, including the freedom of expression, the right to information and intellectual property rights. It must dovetail with other laws geared to ensuring the protection of individuals. It must be compatible with increasing individual mobility, market globalisation and the opportunities provided by new technologies. Perhaps rights may be changed (for example: access rights may change to emphasise the online world and new rights might be added, for example: the right to be left alone, the right to accountability or the right to privacy by design.

- The concept of accountability means that the obligation flows with the information – a useful paradigm for global systems and global data flows. It may be accomplished with tools, practices, contracts etc. and no just by relying on local law.

- The Madrid resolution of data protection authorities on International privacy standards has been very useful guide for developing countries that do not have active data protection laws but needs specific provisions regarding cross-border jurisdiction and conflicts of laws.

- Privacy by design – technology is not a silver bullet – privacy by design is a concept of people, processes, practices and technology – need to look at all those aspects to have privacy by design – privacy needs to be designed in from the very beginning.

- Industry self-regulation can compliment regulation – it can be more flexible and more up-to-date.

- Search engines should be instruments of freedom, accurate and accessible democratic knowledge. In order to assure this, it is important to include Intermediary Liability Exceptions for intermediary services providers in new revised privacy principles.