INTERNET SOCIETY SUBMISSION TO THE OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS IN RESPONSE TO THE CONSULTATION ON THE RIGHT TO PRIVACY IN THE CONTEXT OF THE UN GENERAL ASSEMBLY RESOLUTION 68/167

DATE: 1 APRIL 2014

Question 5 - Any information on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data.

Introduction

The Internet Society respectfully wishes to emphasis that domestic and extraterritorial surveillance encompasses monitoring and interception by commercial, governmental and/or entities of communications, data and/or metadata. Our focus is on surveillance of Internet users.

Merely because Internet communications and data are not encrypted or otherwise protected or obscured does not mean the sender or the intended recipient(s) consider that data to be public. Furthermore, even where communications and data are publicly accessible, individuals may quite reasonably expect that such data would not be used by others in a different context and/or for a different purpose (e.g. for surveillance).

It is also important to be mindful when considering the state of art regarding "the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale" that the surveillance tools and techniques, which today may only be available to a select group of states or entities, could rapidly become resources that anyone could access and use.

Data that has been collected may be stored for indefinite periods of time and over time easily linked with more and larger data sets. Data that is considered meaningless noise could one day be rendered meaningful through developments in data analytics. Data that is currently safe from decryption may not remain protected forever: future decryption techniques may be successful in rendering the data in "clear text".

While an individual's right to privacy must, in appropriate circumstances, give way to matters of public interest such as safety, law enforcement and security, recent events have demonstrated that concepts such as "necessary", "proportionate" and "reasonable" used to determine whether an exemption or lower level of protection is justified need to be revisited. Further, the standard that the international community should apply is not one of strict legality, but rather what is lawful, just and fair.

The Internet Society calls upon the global community to work together to:

- confine the ambit of data collection for national security purposes to those truly exceptional instances where the public interest objectively outweighs an individual's right to privacy; and
- agree a set of strong principles for ethical data handling.

Some initiatives from the Internet technical community

The Internet Engineering Task Force (IETF) and the World Wide Web Consortium have implemented initiatives to specifically address privacy and security in Internet standards development. For example, the IETF, through the Internet Architecture Board (IAB) Privacy Program, published RFC 6973 "Privacy Considerations for Internet Protocols"[1] and the W3C is developing similar guidance for Web standards through the Privacy Interest Group. The IAB Privacy Program also held a privacy tutorial entitled "Engineering Privacy into Internet Protocols" at IETF89 (in London, March 2014).

The disclosures concerning the nature and extent of government surveillance of Internet users' communications and data drew the world's attention to a new threat model: pervasive surveillance and interception of private communications. The IETF and W3C have responded with initiatives to develop standards that strengthen the Internet against this type of threat. For example, the IETF launched a new public email list (perpass@ietf.org) to discuss specific technical proposals for improvements in IETF protocols for better mitigation against pervasive monitoring. Importantly, IETF mailing lists and meetings are open to everyone. The IETF also reached consensus at IETF88 (in Vancouver, November 2013) to address pervasive surveillance as a community in all its standards-track specifications. In early 2014, the W3C and IAB held a joint workshop on "Strengthening the Internet Against Pervasive Monitoring" (STRINT)[2]. The program committee received more than 60 paper submissions across a broad range of topics. Approximately 100 individuals were invited to participate. A report will be made available in due course.

The policy community

The surveillance disclosures have caused ripples across the Internet policy landscape. Many institutions, organisations and communities involved in Internet policy development or dialogue have reacted in one way or another. For the assistance of the OHCHR in preparing its report, we note some examples here:

- UN General Assembly Resolution: *The right to privacy in the digital age*[3]
- *Joint Declaration on surveillance programs and their impact on freedom of expression* (UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights[4] (21 June 2013)
- Council of Europe Declaration of the Committee of Ministers on *Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies*[5] (11 June 2013)
- Message from the Council of Europe Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) to the Council of Europe Committee of Ministers[6] (from the plenary, 15-18 October 2013)

[1] https://tools.ietf.org/html/rfc6973
[2] https://www.w3.org/2014/strint/
[3] http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1
[4] http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&IID=1
[5] (in progress before the Snowden disclosures)
https://wcd.coe.int/ViewDoc.jsp?id=2074317&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383
[6] http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD%282013%29RAP30Abr_rev_En.pdf (page 18)

- Conference of Ministers responsible for Media and Information Society, Political *Declaration: Freedom of Expression and Democracy in the Digital Age Opportunities, rights, responsibilities*[7]
- European Commission documents "Restoring Trust in EU-US data flows"[8]
- European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)[9]

In December 2013, the Council of Europe Cybercrime Convention Committee (T-CY) decided to put on hold its earlier decision[10] to commence work on a protocol regarding transborder access to data[11].

Additionally, there is a whole body of recent and/or ongoing international and regional policy work regarding privacy that is relevant because it defines principles for the collection, handling and cross border access/transfer of personal data. While that work may not be confined to the surveillance context, that work is, naturally, informed and influenced by the now well-known threat of pervasive extraterritorial surveillance of Internet communications for national security or other purposes.

For the assistance of the OHCHR in preparing its report, we note some examples here:

- Organisation for Economic Co-operation and Development (OECD)
    - In 2011, the Organisation for Economic Co-operation and Development (OECD) published *The Evolving Privacy Landscape: 30 Years After The OECD Privacy Guidelines* and commenced its review of the guidelines.[12] Two years later, in 2013, the OECD adopted a *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)* revising the *OECD Privacy Guidelines*.[13]

- Council of Europe
    - The Council of Europe Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) prepared proposals for the modernisation of the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108) and an accompanying supplementary explanatory memorandum.[14] This proposal is being considered by the Ad Hoc Committee on Data Protection (CAHDATA)[15], set up by the Council of Europe Committee of Ministers.

---

[7] http://www.coe.int/t/dghl/standardsetting/media/belgrade2013/Belgrade%20Ministerial%20Conference%20Texts%20Adopted_en.pdf
[8] http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm
[9] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=EN&ring=A7-2014-0139
[10] At the 9th plenary (see page 15 of http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%2922_PlenAbrMeetRep_V9.pdf)
[11] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%2928_Plen10AbrRep_V3.pdf
[12] Please see Chapter 2 at http://www.oecd.org/sti/ieconomy/49710223.pdf
[13] http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf
[14] http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp
[15] http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/Terms%20of%20reference%20-%20Ad%20hoc%20committee%20on%20data%20protection%202013.pdf

- In 2013, Uruguay became the first non-Council of Europe member to accede to the Convention. Morocco has also been invited to accede.[16]

- International Conference of Data Protection and Privacy Commissioners
  - In 2009, the 31st International Conference of Data Protection and Privacy Commissioners ("Conference") produced a *Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data* ("the Madrid Resolution").[17] In 2010, the 32nd Conference adopted a *Resolution calling for the organisation of an intergovernmental conference with a view to developing a binding international instrument on privacy and the protection of personal data*[18]. In 2013, the 35rd Conference adopted a *Resolution on anchoring data protection and the protection of privacy in international law*.[19]

- Asia-Pacific Economic Cooperation (APEC)
  - In 2011, Asia-Pacific Economic Cooperation (APEC) leaders approved the APEC Cross Border Privacy Rules (CBPR) system, a voluntary accountability-based system to facilitate privacy-respecting data flows among APEC economies.
  - There are currently two APEC member economy participants: USA and Mexico. Japan has also applied to join the APEC CBPR system.

- European Commission
  - In 2012, the European Commission proposed a comprehensive reform of the European Union's data protection rules. In March 2014, the European Parliament voted in favour of a proposed regulation[20]. The proposed regulation is currently under consideration by the European Council of Ministers.

- Organization of American States (OAS)
  - On 6 June 2013, during the 43rd Regular Session of the General Assembly of the Organization of American States (OAS) adopted *Resolution 2811 (XLIII-O/13) Access to Public Information and Protection of Personal Data*.[21] Among other things, the resolution instructed the "… Inter-American Juridical Committee to prepare proposals for the [Committee on Juridical and Political Affairs] on the different ways in which the protection of personal data can be regulated, including a model law on personal data protection, taking into account international standards in that area". In making this resolution, the OAS General Assembly took note of the Inter-American Juridical Committee's (IACJ) proposed *Statement of Principles for Privacy and Personal Data Protection in the Americas*[22].

- African Union and UN Economic Commission for Africa
  - The African Union with the UN Economic Commission for Africa is working on a draft convention, currently titled "Draft African Union Convention on the Establishment of a Legal Framework Conducive to Cyber Security in Africa" or "Draft African Union Convention on the Confidence and Security in Cyberspace".

[16] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=&CL=ENG
[17] http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf
[18] http://privacyconference2011.org/htmls/adoptedResolutions/2010_Jerusalem/2010_J3.pdf
[19] https://privacyconference2013.org/web/pageFiles/kcfinder/files/5.%20International%20law%20resolution%20EN%281%29.pdf
[20] http://europa.eu/rapid/press-release_MEMO-14-186_en.htm
[21] http://scm.oas.org/doc_public/ENGLISH/HIST_13/AG06222E04.doc
[22] http://www.oas.org/en/sla/iajc/docs/ijc_current_agenda_privacy_personal_data_protection.pdf

Part II of that draft convention covers "personal data protection" and aims to provide a legal framework for the region, leveraging internationally recognised best practices.

- UNESCO
  - In 2012, the UN Educational, Scientific and Cultural Organization (UNESCO) published a Global Survey on Internet Privacy and Freedom of Expression.[23] UNESCO's aim in publishing the report was to "…provide UNESCO Member States and other stakeholders, national and international, with a useful reference tool". In the foreword, UNESCO said "It is our wish that this publication will contribute to bringing stakeholders together for informed debate on approaches that are conducive to privacy protection without compromising freedom of expression".

- IGF
  - "Security, Openness and Privacy" has been one of the main themes of the Internet Governance Forum (IGF) since 2009. In addition to main sessions devoted to this theme, participants have organised numerous multistakeholder workshops on a range of current and emerging privacy topics.

CONTACT INFORMATION

- Ms. Christine Runnegar, Director, Public Policy, Internet Society (runnegar@isoc.org)
- Mr. Nicolas Seidler, Policy Advisor, Internet Society (seidler@isoc.org)

[23] http://unesdoc.unesco.org/images/0021/002182/218273e.pdf