MEETING REPORT

Improving Data Privacy & Security in ICT4D

A Workshop on Principle 8 of the Digital Development Principles

May 8, 2015
UN Headquarters, New York

TABLE OF CONTENTS

BACKGROUND

Introduction

Ever-increasing global connectivity, and the affordability of Information and Communication Technologies (ICT), have radically modified the way that private corporations, governments and individuals operate. These new technologies have created unprecedented economic development and increased global social welfare, but have also changed the way that democracy works, impacting interactions between citizen and governments.[1] Furthermore, the ICT revolution has, to a large extent, affected the way development and humanitarian policies are designed and implemented. These new technologies, in addition to allowing the collection of an almost unlimited volume of data in a very short timeframe (or in real time), improve data quality by avoiding reliance on self-reported information.

The benefits of using ICT for development are not limited to improved analysis. ICT also provides the means for a more targeted, more appropriate, and more efficient response to crises affecting vulnerable populations.

However, the use of ICT for development also comes with challenges. First, even if the discrepancies between countries in the availability and affordability of new technologies are beginning to shrink, [2] the risk of excluding and increasing the vulnerability of already-marginalized people by relying too heavily on technologies for development remains considerable. It is essential to close the digital divide by transferring technologies, creating infrastructure, implementing training programmes and, in countries where the information is controlled, to increase the flow of free information.

The use of ICT for development faces another challenge: greater use of technology increases the risks of online criminal activity and of illegal interceptions of data from citizens, businesses and members of government by foreign government, businesses and individuals.

These risks – if they should always be examined – can be mitigated, and may be greatly outweighed by the opportunities that ICT offers to achieve inclusive and equitable economic growth and sustainable development. The United Nations has a pivotal role to play, not only in promoting and furthering ICT access and quality, but also in harnessing every benefit of these technologies.[3]

Big Data for Development - Opportunities

Big Data is one of the most promising technological tools for development that has emerged in recent years. It is being used by corporations and governments, but also by international institutions – including the World Bank and other UN entities – to promote and enhance development[4]. For instance, Big Data has been used to track inflation online, to estimate and predict changes in GDP, to monitor traffic, and even to understand disease outbreaks.[5] Analyzing people's opinions through social media has established new ways to measure welfare, while e-mail and Twitter data can be used to study internal and international migration.[6] Finally, mobile network data has been demonstrably valuable for urban planning[7] and to study socioeconomic levels.[8]

[1] General Assembly resolution 68/L.40, *Information and communications technologies for development*, A/C.2/68/L.40 (7 November 2013).
[2] World Bank. *Media (R)evolutions: Global Internet Use*, (Sept. 10, 2015), available at blogs.worldbank.org/publicsphere/media-revolutions-global-internet-use

[3] OCHA, *Humanitarianism In The Network Age*, OCHA Policy and Studies Series, (2013), 39
[4] World Bank, *Big Data in Action for Development,* 2014, http://live.worldbank.org/sites/default/files/Big%20Data%20for%20Development%20Report_final%20version.pdf
[5] Big Data for Development: Facts and Figures, (Sept. 10, 2015), available at http://www.scidev.net/global/data/feature/big-data-for-development-facts-and-figures.html
[6] *Ibid.*
[7] Rohan Samarajiva, *Using Mobile-network Big Data for Urban and Transporation Planning in Colombo*, available at http://www.iesl.lk/Resources/Documents/My%20Docs/Event%20PDF/PL%20L%2016012015.pdf
[8] Big Data for Development: Facts and Figures, (Sept. 10, 2015), available at http://www.scidev.net/global/data/feature/big-data-for-development-facts-and-figures.html

Big Data is an umbrella term that refers to a volume of both structured and unstructured data that is so large that it is difficult to process with traditional database and software techniques.[9] Big Data plays a crucial role in development and humanitarian policies, as it provides a better understanding of the intervention context and enables a better response. In an increasingly 'volatile' world, it can act as a 'digital smoke signal,' giving current information on the vulnerability of a given community. In addition, Big Data is a way to get real-time feedback on the effectiveness of policy actions, which can lead to a more agile and adaptive approach to international development and ultimately to greater resilience.[10]

Like every disruptive technology, Big Data presents game-changing opportunities but also has its challenges.

One of the most prominent challenges to overcome is the absence of data-intrinsic meaning. Data has to be analyzed and given a sense to be converted to actionable information. It is essential that Big Data be put in a context that considers data provenance and the cultural origin of data to avoid bias.

The availability of data poses another challenge. Governments and corporations hold an enormous wealth of data: however, if made available, it could also serve humanitarian and development action.

Last but not least, many argue that the use of Big Data poses a threat to privacy.[11] Maintaining the confidentiality of information, from the data acquisition and storage stage to retention, use, and presentation, it is more important in development and humanitarian contexts than in any other field. Ensuring that information collected and used cannot be tracked back to the individual is therefore essential to protect his "right to be let alone,"[12] but also to protect his life.

The threat that Big Data poses to privacy is not immediately apparent, as the data collection and analysis process does not necessarily include personal data or personally identifiable information (PII)[13]. The privacy risk lies in the fact that Big Data has expanded the range of data that can be personally identifiable. Through the use of metadata such as a set of predictive and aggregated findings, or by combining previously discrete data sets, analysis of Big Data can produce novel PII. These PII are usually not created at the point of collection, or even during the most significant data transfers, and numerous data collections and transfers can occur before any harm can be predicted. In addition, over the past few years, computer scientists have repeatedly shown that even anonymised data can be re-identified and associated with specific individuals under certain circumstances.[14]

Even more problematic is the fact that current privacy protections often do not take Big Data into consideration, as the existing regulatory schema appears incapable of keeping pace with this technology.[15] The questions of security breach, data ownership, and who is responsible if the data is misused also must be carefully considered.[16]

Despite the risks of using Big Data, privacy in the digital age[17] should not be considered an obstacle to this use. For instance, it has been shown that not every treatment to make data

[9] United Nations Global Pulse (May 2012), *Big Data for Development: Challenges & Opportunities,* 13.
[10] *Ibid.*
11 Privacy defined by the International Telecommunication Union as "the right of individuals to control and influence what information related to them may be disclosed."

[12] Warren Samuel and Brandeis, Louis. *The Right To Privacy*, 4 Harv. L. Rev. 193 (1890), 205.
13 For the purposes of this document, we will use the term PII
[14] See Narayanan Arvind and Shmatikov Vitaly, *Robust De-anonymisation of Large Sparse Datasets*, 2008, IEEE Symp. On Security & Privacy, 111, Available at https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf
[15] Crawford, Kate and Schultz, Jason, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, Boston College Law Review, Vol. 55, No. 93, 2014, 94, available at: http://ssrn.com/abstract=2325784
[16] OCHA, *Humanitarianism In The Network Age*, OCHA Policy and Studies Series, (2013), 40.
[17] United Nations, International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 entry into force 23 March 1976, in accordance with Article 49. See also, UNGA, *The right to Privacy in the Digital Age*, 18 December 2013, UN Doc A/RES/68/167.

less identifiable makes the data less useful.[18] However, the appropriate legal framework, ethical guidelines, and technological solutions should be implemented. Even though the global regulatory privacy framework is fragmented, certain principles – such as the OECD guidelines – are widely acknowledged and applied.[19] Global development and humanitarian sector professionals must integrate key principles of user consent, transparency of data collection, proportionate use, and minimization into all stages of their programmes.

UN GLOBAL PULSE

In 2009, the United Nations Secretary-General established the Global Pulse initiative. The impetus for Global Pulse arose from the recognition that digital data offers an opportunity to gain a better understanding of changes in human well-being and real-time feedback on how well policy responses are working.[20]Global Pulse is located on three continents (with its headquarters in New York and offices in Jakarta and Kampala). In order to more accurately understand the circumstances of vulnerable populations and to give an appropriate and useful meaning to the data collected, the ultimate goal is to help decision-makers improve their responses based on this knowledge.

Respecting and valuing individuals' privacy is a cornerstone of Global Pulse's work. In its commitment to privacy, Global Pulse follows Data Privacy Guidelines and Data Privacy Principles.[21] To ensure transparency and inclusive process and participation, it has established a Privacy Advisory Group. The Privacy Advisory Group is comprised of global experts from various sectors to to stimulate continuous dialogue on critical topics related to data protection and privacy[22].

DIGITAL DEVELOPMENT PRINCIPLE 8 WORKSHOP

On 8 May 2015, Global Pulse hosted a workshop on data privacy and security in technology-enabled development projects and programmes. This workshop was part of a series of events focused on the Nine Principles for Digital Development.[23]

The Principles for Digital Development (http://digitalprinciples.org) are guidelines that can help development practitioners to integrate established best practices into technology-enabled programmes. They are written by and for international development donors, multilateral organisations, and implementing partners, and they are freely available for use by all.

Principle 8 ("Address Privacy & Security") proposes that ICT4D programmess should: *assess and mitigate risks to the security of users and their data; consider the context and needs for privacy of personal data when designing solutions; ensure equity and fairness in co-creation; and protect the best interests of the end-users.*[24]

The workshop was held at the UN Headquarters in New York, and was designed to encourage an exchange of expertise and practical experience in the field of data privacy and data security. Colleagues from UN Agencies, development practitioners, and experts from academia and the private sector attended and participated in the discussions.

[18] UN Global Pulse, *Mapping the Risk-Utility Landscape: Mobile Data for Sustainable Development & Humanitarian Action*, Global Pulse Project Series no. 18, 2015, 3.
[19] Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980), available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
[20] United Nations Global Pulse (2013) *Big Data for Development: A primer,* available at http://www.unglobalpulse.org/sites/default/files/Primer%202013_FINAL%20FOR%20PRINT.pdf
[21] Global Pulse Privacy Principles. (Sept. 10, 2015), Available at http://www.unglobalpulse.org/privacy-and-data-protection
[22] Global Pulse Privacy Advisory Group. (Sept. 10, 2015), available at http://www.unglobalpulse.org/data-privacy-advisory-group
[23] Principles for Digital Development, (Sept. 10, 2015), available at http://digitalprinciples.org/
[24] Principle 8: Address Privacy and Security, (Sept. 10, 2015), available at http://digitalprinciples.org/address-privacy-security/

The event included two interactive discussion sessions on data privacy and security, followed by breakout groups focusing on real-world applications and challenges related to putting Principle 8 into practice.

9 PRINCIPLES FOR DIGITAL DEVELOPMENT

The Principles for Digital Development find their roots in the efforts of individuals, development organisations, and donors alike who have called for a more concerted effort by donors and implementing partners to institutionalize lessons learned in the use of information and communication technologies (ICTs) in development projects.

1. ***Design with the user***
2. ***Understand the ecosystem***
3. ***Design for scale***
4. ***Build for sustainability***
5. ***Be data driven***
6. ***Use open data, open standards, open source, open innovation***
7. ***Reuse and improve***
8. ***Address privacy & security***
9. ***Be collaborative***

For more information, visit http://digitalprinciples.org/about/

The driving goal of this workshop was to bring together diverse opinions and expertise to examine potential approaches to a data privacy and protection framework for ICT4D programmes. The objective was to further refine the existing understanding of privacy and data security concepts, and to exchange experiences and common challenges in – and solutions for – incorporating data-securing and privacy-protecting measures into development programmes.

SESSION 1: DATA PRIVACY POLICIES

This session focused on data privacy from a policy perspective, examining organisational accountability and responsible information governance.

Key Data Privacy Policy Challenges Addressed

Fragmented Regulatory Landscape

Data privacy and protection has undoubtedly become a global issue as cross-border humanitarian crises become more frequent and technology continues to tear down international barriers. One of the biggest challenges in the area of privacy policy is a lack of global consistency in the interpretation of various terms and guidelines included in data protection laws. This lack of consistency makes it difficult for international organisations and companies to adjust their privacy practices to the differing regulations around the world. Moreover, the lack of unified and clear guidance on data privacy and data protection globally, creates challenges in humanitarian response cases.[25]

In 2011, the International Conference of Data Protection and Privacy Commissioners encouraged governments to adopt laws to allow the use of personal data during major natural disasters.[26] Some jurisdictions have created provisions that allow government agencies to share information with authorized humanitarian actors following an emergency or disaster. To date, the majority of countries do not have such explicit exceptions.[27]

The international community has started to take a proactive stance in addressing the issues surrounding the Internet of Things, Big

[25] OCHA, *Humanitarianism in the Age of Cyber-warfare – Towards the Principled and Secure Use of Information in Humanitarian Emergencies*, OCHA Policy and Studies Series, October 2014, 011, available at https://docs.unocha.org/sites/dms/Documents/Humanitarianism%20in%20the%20Cyberwarfare%20Age%20-%20OCHA%20Policy%20Paper%2011.pdf

26 General Assembly resolution, *Data Protection and Major Natural Disasters*, 2011/GA/RES/004 (1 November 2011). available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/11-11-01_Mexico_Natural_Disasters_EN.pdf

[27] Reidenberg, Joel R., Gellman, Robert, Debelak, Jamela, Elewa, Adam, and Liu, Nancy. *Privacy and Missing Persons After Natural Disasters*, Washington, DC and New York, NY: Center on Law and Information Policy at Fordham Law School and Woodrow Wilson International Center for Scholars (2013), 11

Data, and associated risks and harms. The recent UN Resolutions and June 2014 report of the UN High Commissioner for Human Rights on the Right to Privacy in Digital Age stressed the importance of considering the risks to human rights that the uncontrolled use of personal information poses.[28]

MAIN RECOMMENDATIONS FROM SESSION 1 (DATA PRIVACY POLICIES):

Adhere to the basic principles of privacy: Organisations should be proactive, not reactive, when addressing privacy. Privacy mechanisms should be built from into the design of a project from the start. Organisations should be transparent about how data is collected and used. They should be responsive to concerns and queries.

Maintain the purpose for data: Ensure that personal data is being used for a specific, fair, and justified purpose. Data collection and use should be necessary and proportionate to the identified and consented-to purpose.

Transparency should be an ongoing commitment: Transparent policies should be implemented so individuals know how their data is collected and used. Individuals should be informed of data collection, use, sharing practices and retention duration.

Consider the principle of minimization: Organisations should consider the principle of minimization, which dictates that data processors collect only essential data, keep data for the minimum possible time, and destroy the data when its no longer needed.

The UN's appointment of a Special Rapporteur on the Right to Privacy also highlights the organisation's role in promoting and protecting the right to privacy worldwide. For example, the 36th International Privacy Conference called for international enforcement cooperation, and the goal of the 37th International Privacy Conference[29] (to be held in October 2015) is to "build bridges" globally for safer and more responsible data use.

User Control and Consent

User consent is one of the key principles of privacy regulations throughout the world. The principle implies that users are entitled to have control over their personal data.[30]

Organisations must explain their data processing activities and obtain consent from individuals; individuals must read and understand complicated privacy disclosures, and express their "informed" consent.[31] The act of consent has been perceived as legitimizing the collection, use, or disclosure of personal data. However, there are a number of problems with the consent justification, and on the whole, the power of consent does not seem to actually provide people with meaningful control over their data.[32]

Studies have shown that people are not able to make informed and rational decisions about whether they should consent to the various uses of their personal data.[33] Most people do not read the privacy policies, as they are often too long and difficult to understand.[34] Even when privacy policies have been shortened and simplified, reader comprehension did not improve much.[35] One explanation could be that people do not adequately assess the consequences of agreeing to certain uses of their data.[36] Development programmes must consider whether or not a subject's consent is valid if the subject does not actually understand the conditions with which he or she is agreeing

[28] UNGA, *The right to Privacy in the Digital Age*, 18 December 2013, UN Doc A/RES/68/167.
[29] The International Privacy Conference, 2015, available at https://www.privacyconference2015.org.

[30] Joergensen, R., *The unbearable lightness of user consent,* Internet Policy Review, (2014). 3(4), available at http://policyreview.info/articles/analysis/unbearable-lightness-user-consent.
[31] Cranor Lorrie & McDonald Aleecia, *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society, 2008, available at http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf
[32] Solove Daniel J., *Privacy Self-Management and the Consent Dilemna*, 126 Harvard Law Review 1880 (2013), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.
[33] *Ibid.*
[34] Anton Annie I., Earp Julia B., He Qingfeng, Stufflebeam William, Bolchini Davide, Jensen Carlos, *Financial Privacy Policies and the Need for Standardization*, IEEE Security and Privacy, v.2 n.2, p.36-45, March 2004, available at http://dl.acm.org/citation.cfm?id=1437405&CFID=544623824&CFTOKEN=35810549.
[35] Calo M. R., *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV.1027 (2013). Available at: http://scholarship.law.nd.edu/ndlr/vol87/iss3/3.
[36] *Ibid.*

to. Moreover, there exists ongoing debate on whether the need for emergency humanitarian aid should waive the need for consent.[37]

Lack of Transparency

Humanitarian and development programmes are often supported by the international community and by donors. Both donors and organisations recognize that transparency is key for accountability and greater effectiveness in furthering their causes. Therefore, it is important for these organisations to gain the trust of their supporters and the communities they are trying to help. When a vast quantity of information is being collected, it is easy for organisations to lose sight of what is actually being collected, and why that collection is necessary.

Publicized privacy policies and privacy notices may be the key to effective transparency, which is needed for building community trust in the use of ICT for development.

Re-identification Risk

Data that have been processed, enhanced, or changed by Big Data programmes may have both internal and external benefits for organisations. Often, the data must be anonymised to protect the privacy of the individual whose data was originally collected.

The "mosaic effect" increases the significance of choosing the proper approach when anonymising or aggregating data. The "mosaic effect" occurs when "the information in an individual dataset, in isolation, may not pose a risk of identifying an individual, but when combined with other available information, could pose such risk."[38] Data that is not properly anonymised and secured may compromise data privacy: such data can be combined with other datasets, including geo-location, image recognition, and behavioral tracking, leading to re-identification.[39] Possible correlations between data subjects contained within separate datasets must be evaluated, as third parties with access to several datasets may be able to re-identify otherwise anonymous individuals.

For example, "anonymised data" collected from movie rentals was shown to be easily "de-anonymised," identifying a known individual by correlating the rental dates of as few as three movies with the dates of posts on an online movie platform.[40] Other research on call detail records has found that record location and time could be re-identified to recognize a specific individual.[41] In 2014, the New York City Taxi Commission released a dataset that detailed every taxi ride in 2013, including pickup and drop off times, locations, fares, and tip amount, as well as anonymised versions of the taxi's license and medallion. One hacker was able to de-anonymise all the data, which could now be used to calculate, for example, the driver's annual income. People could also now use the data to identify where a specific individual went, how much they paid, weekly habits, and other private details.[42] To prevent these types of incidents, development progammes must ensure that the datasets being used are properly anonymised and cannot be re-identified.

Key Highlights from Presentations on Data Privacy Policies

[37] Reidenberg, Joel R., Gellman, Robert, Debelak, Jamela, Elewa, Adam, and Liu, Nancy. *Privacy and Missing Persons After Natural Disasters*, Washington, DC and New York, NY: Center on Law and Information Policy at Fordham Law School and Woodrow Wilson International Center for Scholars (2013), 11.

[38] OCHA, *Humanitarianism in the Age of Cyber-warfare – Towards the Principled and Secure Use of Information in Humanitarian Emergencies*, OCHA Policy and Studies Series, October 2014, 011, available at https://docs.unocha.org/sites/dms/Documents/Humanitarianism%20in%20the%20Cyberwarfare%20Age%20-%20OCHA%20Policy%20Paper%2011.pdf.

[39] Hassan Wael, *Five Key Big Data Privacy and Information Protection Challenges*, Oct 8, 2014, available at https://www.linkedin.com/pulse/20141008182836-23177158-five-key-big-data-privacy-and-information-protection-challenges.

[40] Big Data for Development: Facts and Figures, (Sept. 10, 2015), available at http://www.scidev.net/global/data/feature/big-data-for-development-facts-and-figures.html.

[41] *Ibid.*

[42] Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset, (Sept. 10, 2015), available at http://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/.

Presentation by Micah Altman, Director of Research and Head of Programme on Information Science, MIT:

- The core concepts of data privacy are: *confidentiality, information security, sensitivity, and identifiability.* Confidentiality deals with how we control access to information, whereas information security concepts are concerned with control and with creating mechanisms for disclosure within information systems. There are three different types of identifiability: (1) a "Where's Waldo" type, which offers the least protection; (2) a "hiding in the crowd" type that allows distinguishability; and (3) a type that asks what new information could be learned about somebody specific, even if one cannot necessarily identify them by name.
- Some of the main overarching frameworks for data privacy are: *privacy by design, fair information practice, and the OECD principles.*

Presentation by Peter Micek, Senior Policy Counsel, Access Now:

- Surveillance is about power and control; it's not necessarily about privacy. Privacy is not about something that you need to hide; it is the freedom to express and the ability to control.
- The trust and safety of marginalized and vulnerable communities are at risk. In these communities, trust is already in short supply. Privacy enables the exercise of human rights, and trust in institutions and societies.

Presentation by Mila Romanoff, Legal & Data Privacy Specialist, UN Global Pulse:

- To unlock the use of Big Data for public good, there is a need to catalyze the global development and humanitarian community in an effort to ensure data protection and safeguard privacy.
- An important component of each data related project is conducting a privacy risk assessment (PIA). Purpose Justification and Principle of proportionality are very critical for a successful PIA analysis. It is , however, to not only assess the likelihood and magnitude of possible risks and harms, but also to ensure that benefits, their likelihood, and their potential beneficiaries are considered.
- Consent and commitment to not re-identifying previously anonymised data are critical.

Presentation by Kathy Joe, Director of International Standards & Government Affairs, European Society for Opinion and Market Research (ESOMAR):

- Privacy by design should be implemented in every project. Privacy is not just a set of rules: it is an attitude. It is not something that we have to do, but it's something we want to do in order to maintain consumer trust. Default privacy settings need to be embedded into the programmes.
- Research companies need to be mindful of security practices. Training is absolutely essential and should be implemented throughout the company.

SESSION 2: DATA SECURITY PRACTICES

This session focused on best practices and mechanisms for information security, from a data engineering standpoint. Participants shared examples and best practices from their own organisations in developing a secure IT environment for safe information handling.

Key Data Security Challenges Addressed

Data security was once the domain and concern of IT departments. However, because of advanced technology and Big Data use, new regulations and policies have made data security a concern for all types of

organisations.[43] Organisations and companies have many laws, regulations and standards with which they must comply, but the ambiguity of the rules leaves much of the design and implementation of the regulations at the organisation or company's discretion. In doing so, it forces organisations and companies to mold their own data security compliance, and to constantly assess and redesign the rules to suit their changing risk landscape and evolving data needs.[44]
As large data breaches are becoming more prevalent, organisations are looking for ways to revamp their security practices to focus on prevention. Consequently, they must simultaneously employ preemptive measures to mitigate the risk of a breach and maintain an incident response plan for when one inevitably does. The data collector must take all technical and organisational measures necessary to ensure the security and confidentiality of the personal data, so as to avoid its alteration, loss, or unauthorized access or treatment.[45] Data should be secured to prevent unintended uses, including the security of the channels by which the data is collected; the places, virtual or physical, where the data is stored; and of the tools used to exchange data between organisations.[46] While organisations cannot predict when or how a breach will occur, they can be prepared when one does occur.

Lack of Resources

Implementing data security in the humanitarian and development field does not come without challenges. Many development programmes simply do not have the financial resources or manpower to allocate time and money to data security. Additionally, donors or the state may have a great influence over certain organisations, which are unable to ignore the interests of their benefactors. These sponsors usually do not consider data security a high priority and often feel that resources would be better utilized in other areas. If they do support better data security practices, it usually boils down to the most basic best practices to ensure being able to pass a regulatory audit.

Big Data Governance

The implementation of Big Data initiatives may lead to the creation of previously confidential or sensitive information through data aggregation. Development programmes that implement Big Data initiatives without a strong governance regime in place, puts themselves at risk. Therefore, a strong ethical code, along with established data security process, training, people, and metrics, is imperative to govern use of Big Data in ICT4D.

Original Intent

Data should be collected for a specific, legitimate purpose and only data needed for that purpose should be collected.[47] Development programmes must make sure that all privacy and security requirements that are applied to their original data sets are tracked and maintained across the information life cycle from data collection to disclosure or retention. Following this principle will increase the likelihood that datasets will remain in a secure network and spare the risk of data re-identification by aggregation.

Third Parties

The use of third parties in developing technology applications or tools has become more frequent as organisations outsource certain operations. However, the outsourcing of data security practices to third-party organisation may not be adequate. Therefore, it is critical for development programmes to conduct proper due diligence and vet potential partners in the outsourcing process.

[43] Cronin Kevin, *Best Practices and the State of Information Security*, 84 Chi.-Kent. L. Rev. 811 (2010), available at: http://scholarship.kentlaw.iit.edu/cklawreview/vol84/iss3/8
[44] *Ibid.*
[45] DLA Piper - Data Protection Laws of the World , (Sept. 10, 2015), available at http://dlapiperdataprotection.com/#handbook/world-map-section
[46] OCHA, *Humanitarianism in the Age of Cyber-warfare – Towards the Principled and Secure Use of Information in Humanitarian Emergencies*, OCHA Policy and Studies Series, October 2014, 011, available at https://docs.unocha.org/sites/dms/Documents/Humanitarianism%20in%20the%20Cyberwarfare%20Age%20-%20OCHA%20Policy%20Paper%2011.pdf
[47] *Ibid.*

Such processes must include consideration of that company's data security processes and frameworks. For example, some organisations may request to be provided with a data security certificate.

Lack of Unified Approach to Data Security

The fragmented regulatory landscape, the lack of commonly accepted data security practices, including anonymisation standards, makes it highly difficult for the development agencies to implement data security in their global projects, but also to gain access to data in certain cases, where access is blocked due to a lack of regulatory approved and updated data security methods. To keep current with quickly changing and newly implemented laws, development programmes must perform an initial inventory of applicable laws and technical standards and update their inventory accordingly on a regular basis.

Highlights from Presentations on Data Security

Thomas Braun, Chief of Global Security & Architecture Section, UN Office of ICT:

- There are three technical challenges to address assuming data collection objectives and uses are in place: (1) protecting data from unauthorized users; (2) protecting data from authorized users; and (2) preventing unintended disclosure.
- Most websites and interfaces are vulnerable to attacks, but it is possible to secure websites if security is considered from the beginning. Basic requirements for initial security include: creating strong passwords, conducting penetration tests, and ensuring that the website or interface remains secure through its life cycle.

Clayton Sims, VP of Mobile Development and Head of Research & Development, Dimagi:

- Different organisations and industries have various data security concerns. The challenge is being in scale with all these organisations and offering services for all the different concerns. Data privacy and security have to be tailored to the type and the manner of the data being dealt with.
- Human factors will trump 99% of all security practices that an organisation has.

Gary Fowlie, Head, ITU Liaison Office to UN:

- One of the first steps every responsible person should take is to implement transparent policies regarding the processing of personal data. These policies need to explain the type of data, the data life cycle, who is processing the data, and the processing application
- Cloud computing should be easy for the consumer to use, but the cloud provider and developer should have more complex protocols. There is no universally binding resolution covering all countries in the context of cloud computing. Cloud computing needs to be highly secure but guaranteeing that kind of security and encryption is not always that easy.
- It is essential to use Privacy Enhancement Technologies ("PETs").

BREAKOUT GROUPS

Following the panel sessions, attendees were split into three breakout groups. Each group was asked to consider questions in implementing best practices and policies in various areas of privacy and security.

1) Developing a Risks, Harms and Benefits Framework: The goal of this group was to identify potential risks, harms and benefits, when planning and conducting an ICT4D project. The breakout group, facilitated by Mark Latonero of the Data & Society Research Institute, discussed potential harms, risks and benefits of ICT4D projects. The breakout session started with a case study presented by Cara Wollinsky and Lilian Barajas of UN OCHA.

KEY POINTS FROM "DEVELOPING A GOOD PRIVACY POLICY" BREAKOUT:

Privacy notices and policies should be easy to understand, facilitate comparison, and be actionable. Organisations should articulate how data is being used, who has access to the data, and the potential risk factors that are specific to the development context, such as corruption, ethnic tensions and displacement.

Notice should be accessible and in a language that the public majority can understand. They should be short, use plain language, and be presented in a common format. Organisations should clearly explain their information management practices and make those explanations easily accessible. Data should be used only for a specific purpose and it should be retained for as long as necessary to achieve that purpose. It should not be held indefinitely and should be destroyed when no longer needed.

Finding ways to supplement privacy policies may be less feasible in development programs due to either lack of funding or support; however, an organisations' ability to come up with new and innovative solutions to enhance transparency is not only important for privacy but also for organisations' relationships with the community to the benefit of which an organisation is conducting an ICT4D project.

KEY POINTS FROM "DEVELOPING A RISKS, HARMS & BENEFITS FRAMEWORK" BREAKOUT:

A risks management framework that would include an assessment of risks, harms and benefits may be helpful especially to those who are not data protection experts, as a means to make compliance and obligations more concrete and decide when they are implicated.

When accounting for risks, data users must also assess, prioritize, and quantify a project's benefits in order to understand whether assuming the risk is ethical, fair, legitimate, and cost-effective.

Risk mitigation strategies are essential for protecting privacy, yet at the same time they can constrain beneficial uses of data, thereby minimizing data utility.

If the likelihood of accomplishing a benefit is extremely remote or if the contemplated benefit is minor, large privacy risks would not be justified.

2) **Developing a Good Privacy Policy:** The goal of this group was to identify key points to include in the design of a data privacy policy for the implementation of ICT4D projects. The breakout group, facilitated by Jos Berens of Leiden University, discussed the essential principles and steps to take and consider in a privacy policy. The breakout session started with an example shared by Ms Sheryl-Ann Yamuder of MasterCard.

3) Developing Good Data Security Practices: The goal of this group was to identify best practices, mechanisms and technology solutions in information security in ICT4D projects. The breakout group, facilitated by Enrique Piraces of Benetech, discussed critical information security considerations for building secure apps, maps, and websites.

CONCLUSION

While there are good practices that can be learned and followed, many challenges still remain when it comes to privacy and data protection for development. Development programmes and projects should make the effort to work towards addressing those challenges. The main goal of development programmes is to contribute to the public good. Use of technologies and digital information undoubtedly provides many advantages and benefits for advancement in humanitarian and development work and should therefore be embraced. However, a blind eye should not be cast onto the possible privacy and security risks. With the proper attitude, considerations, and procedures, organisations should try their best to ensure that their work is not compromising the security of the data and data privacy of individuals.

For more information on the Principles for Digital Development, please visit: http://digitalprinciples.org/

And join the conversation on social media using #DigitalPrinciples

For more information on UN Global Pulse, please visit: http://unglobalpulse.org/