IGF 2016 Workshop Report Template

Session Title	On cybersecurity: Who has got our back?
Date	09 December
Time	10:45-11:45
Session Organizer	Global Partners Digital
Chair/Moderator	Sheetal Kumar
Rapporteur/Notetaker	Sheetal Kumar
List of Speakers and their institutional affiliations	Brian Bergstein (MIT Technology Review) Dominique Lazanski (GSMA) Asad Baig (Media Matters for Democracy) Tatiana Tropina (Max Planck Institute)
Key Issues raised (1 sentence per issue):	Encryption: Is strong encryption creating obstacles to law enforcement doing its job re: crime and national security? Network security: How do cybersecurity policy decisions relating to encryption and other related issues (like data retention) impact both human rights and the stability, security and resilience of the internet's underlying infrastructure? Jurisdiction/regime type: The outcomes of specific policies in terms of their impact on human rights and on cybersecurity are complicated by the variety of political systems and legal regimes around the world
If there were presentations during the session, please provide a 1-paragraph summary for each Presentation	Presentation 1 (Dominique Lazanski): described the new challenges faced by operators and the business community due to the different legal requirements in the management of networks, pointing for example to Europe and the NIS. She mentioned that these regulations can and has led to tensions, especially with regards to the 'Internet of Things' where standards are at an early stage (although GSMA has developed a flexible framework for interoperability launched in March 2016 looking at network as well as end-point security). However, there remain challenges when it comes to ensuring both flexibility and security in standards development – including those related to privacy, collection of data, data protection and security. Presentation 2 (Brian Bergstein): began with a consideration of whether access to consumer data by law enforcement agencies should be allowed, stating that the response is broadly 'yes', but with caveats – e.g not all the time and not through bulk surveillance. Access to data must be conducted in accordance with the rule of law in order to protect the right to privacy. However, law enforcement does have legitimate demands when it comes to the need to access consumer data as well as responsibilities. This doesn't come in conflict with our right to use encrypted devices. There is a risk of the gap between the law enforcement and tech companies growing too wide. We need to ask whether we are expecting private sector companies to be the protector of our civil liberties in these debates instead of governments and civic institutions – as citizens we need to safeguard democracy, democratic institutions and the legitimacy of accountability mechanisms. Democracy and civic institutions depend on transparency and the rights to privacy and freedom of expression are not absolute rights – governments need an auditable process that is transparent and open in order to be access consumer data. Without that, other 'behind the door' measures like hacking pose bigger threats to human rights. Technology should strengthen civic institutions. It is not sufficient to only ask whether something is good for privacy but also, whether it is good for democracy, civic engagement and human rights.

	Presentation 3 (Tatiana Tropina): broadly agreed with the points made by Brian Bergstein, reiterating the need to recognise the legitimate demands of law enforcement and the need for safeguards in the access to consumer data. She called for a move away from simplistic debates and stated that there is a need to distinguish between legitimate demands of law enforcement agencies and other access to data. She pointed to the long-standing practice of interception of communications and requirements that data be provided in readable format which has existed as long as phones have been used for criminal purposes. However, law enforcement has been subject to the rule of law/needed a court order to do this. The difference with the FBI/Apple case was that the disclosure of information could 'endanger' everyone. We also need to distinguish between different types of data and for what purposes that data is sought. Tech companies should not provide master keys, backdoors and other technical measures that could result in access to data that is not subject to the rule of law for legitimate purposes. On bulk data collection, the point was made that 'we won't get rid of it' but it should be subject to the strictest safeguards. **Presentation 4 (Asad Baig):** framed the main question as whether there should be legal means for access to data. A weaker encryption system does not work in anyone's interests (as it can be exploited by anyone). He called on the need to consider a 'global perspective' as government is not a 'monolith' and there are a number of governments that can use weaker encryption standards against citizens, for example to attack journalists and human rights defenders. The debate should also be framed not necessarily as a question of privacy but one of 'security', including personal security – a better framing may be of 'security' vs 'security' rather than 'security vs privacy'.
Please describe the Discussions that took place during the workshop session: (3 paragraphs)	**The challenge of competing jurisdictions:** There is a serious challenge when it comes to the way that different regimes use technology and policy measures and how they affect cybersecurity – for example there are democratic governments and then there are authoritarian governments (although there are many types of democratic governments including repressive ones) which will use the same technologies to very different ends with implications for human rights. However, despite popular views to contrary there are certainly existing 'clubs' or agreements between countries – like MLATs which allow for lawful sharing and access of consumer data between countries that are on their own terms and situation-specific. **Roles and responsibilities of technology and software development:** There is a tension here between those who develop technology solutions and those who develop policy solutions– sometimes there are solutions which seem to be proposed which are simply not technically possible (e.g to make technology that works in the hands of some and not others). One audience participant/software developer referred to this as the exasperating demand for "nerds to nerd harder". One example was provided by an audience participant, for example, of a Mexican human rights defender whose phone was hacked into by corrupt police officials who had been co-opted by the drug mafia – and which not only compromised her data but which tragically ended in the loss of her life. However, it is still important to consider what the best policy solutions are in order to support the self-identified limitations of software developers as well as human rights concerns. It is problematic to rely on companies to defend civil liberties as that is not what they are responsible for. Therefore, we need to nurture our civic institutions (as technology can amplify existing human rights challenges like lack of strong democratic institutions in certain countries), and not undermine the rule of law in the process of finding solutions to these issues.

Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways: (3 paragraphs)	Lawful and exceptional access to consumer data is important but only under very strict safeguards that respect the rule of law. However, there are countries where such safeguards do not exist, including in repressive democratic systems. There is therefore a need to develop global norm standards and use policy spaces to ensure that there are commitments made by policymakers which protect encryption and network security and do not undermine human rights. For example, there was discussion of the need to address data retention laws and whether they are effective. In addition, there are governments which have committed to certain positions such as taking a strong stance against backdoors (like the Netherlands) and which may provide way forward in terms of determining what guidelines should inform cybersecurity policy more widely. There is also a real need for more transparency when it comes to data use, data sharing and access to consumer data by law enforcement – this will help private sector actors cooperate with the government in ways that are respectful of the public interest. We also need more examples of where strong encryption has supported human rights, or where weak encryption has compromised rights (such as that of the Mexican HRD mentioned above) and we need to collect and share these widely to inform our policies so that they are human rights respecting. It's not the media or private sector companies 'job' to protect civil liberties and human rights: they may have a role to play but we also need government to be transparent, accountable and have auditable processes. We also need to consider what the wider community can do, for example in terms of supporting and embedding human rights and ethics principles into technology. Finally, in terms of the IGF, it was suggested that this topic requires more intersessional work in order, for example, to identify best practices. Post the workshop, the session organiser will consider and explore the available options for intersessional work (for example, integrating the issues discussed into relevant BPF/Dynammic Coalitions).