IGF 2017 Reporting Template

Session Title:

WS61: Between a rock and a hard place? : Identifying encryption policies that are human rights respecting

Date:

19 December

Time:

17:20-18:20

Session Organizer:

Global Partners Digital (GPD)

Chair/Moderator:

Sheetal Kumar (GPD)

Rapporteur/Notetaker:

Sheetal Kumar (GPD)

List of Speakers and their institutional affiliations:

'Gbenga Sesan, Paradigm Initiative
Nicolas Seidler, Internet Society

Unfortunately two of the women speakers originally confirmed were unable to attend at short notice.

Key Issues raised (1 sentence per issue):

- The crackdown on the use of strong encryption, including by legal means (for example the enacting of of laws which criminalise the use of encryption or which weaken encryption standards) remains a threat to human rights
- The legal frameworks which relate to encryption should also protect human rights because strong encryption is an enabler of human rights and of cybersecurity – in that sense it is mutually "good for business" and for human rights
- The challenges to strong encryption arise in a securitised framework, where there are competing tensions between law enforcement access to information in the course of criminal investigations and the use of strong encryption to routinely protect communications (as deployed in popular communications platforms like mobile messaging apps) – however, this securitised framework provides an imbalanced framing on the issue of encryption

If there were presentations during the session, please provide a 1-paragraph summary for each presentation:

Nicolas Seidler, Internet Society: Encryption policies have the difficult task to address two important, yet sometimes competing policy objectives: 1) Securing infrastructure, communications and data: explain why encryption is so important for all layers of society, including human rights 2) Enforcing law: enabling LE to access communications that are targeted under suspected illegal activity. Perhaps the biggest dilemma facing both law enforcement and companies that provide digital services becomes: how much encryption is "enough" and who gets to decide? In the market, some encryption services are more "law enforcement friendly" than others. In the last four years, some companies have chosen to get rid of their ability to decrypt customers content. This presents a new environment for law enforcement many devices encrypted by default (encryption at rest) and millions of users using end-to-end encryption in messages (encryption in transit). But not all do: e.g. in China, WeChat has encryption in transit, but not on the server side, which allows a level of government access and control. In this context, LE asks have changed over past 4-5 years, from asking for "backdoors", to now focus more on "lawful hacking", while demanding "responsible encryption". This is how the debate is evolving and there are growing asks from law enforcement to companies to circumvent encryption. From Internet Society perspective: the starting point is that encryption should be the norm for Internet traffic and data. Where possible, end-to-end encryption solutions should be made available. Attempts to limit the use of encryption, legal or technical, will have too many negative impacts to security and rights of law-abiding citizens. So how to have encryption policies that reconcile these seemingly competing policy objectives? How much encryption is enough encryption? Can lawful hacking be a solution that leaves the majority of users protected while targeting suspected criminal activity in a more targeted way? In other words, meeting proportionally and necessity requirements? And who gets to decide?

'Gbenga Sesan, Paradigm Initiative: Encryption is important for human rights but we often hear about how it is used for crime – and so we see a crackdown on the use of strong encryption but there are in fact, legitimate and illegitimate ways in which the law can be used. What this means is that you'll see the law used to put people behind bars who shouldn't be there for exercising their freedom of expression, while real crimes go unpunished. There are also legal and technical responses to crime which are not human rights respecting but which should be. What this means is that generally we see a crackdown on free speech, and a lack of transparency. However, in the last few months in Nigeria, there have been conversations around unlikely partnerships and of different stakeholders sitting around together which is necessary as its important to have robust debate and arguments and you can understand others views. What is absolutely necessary in contexts where the law can be abused is a need for clarity of process and a need to respect process, for court order or warrants for example to actually be presented and for these to be clearly for legitimate purposes. We can make the case that human rights are good for business too – that encryption for example is an enabler of security and trust. And finally, citizen awareness is important, people haven't been asking questions as to why should all communications be encrypted end-to-end but they should be. Laws and policies should be human rights respecting and its important for them to be formulated in an inclusive process if they are going to be.

Please describe the discussions that took place during the workshop session (3 paragraphs):

The second part of the workshop (following the panellist interventions which are summarised above) was conducted as an interactive break-out session. Participants broke up into five groups of five-six and were presented with a table of criteria (of suggested human rights respecting approaches to encryption policy) against which to assess de-identified excerpts from real-life laws and policies pertaining to encryption.

Some of these discussions illustrated the nuanced and difficult nature of this debate. For example, a number of the excerpts of laws and policies referred to decryption orders (an increasingly commonly deployed and legislated encryption workaround) and participants disagreed to what extent the safeguards included in these orders were sufficient enough to guard against abuse and to protect human rights. Some commented on the fact that in some countries, with weak enforcement of the rule of law a decryption order may 'be ok' on paper but be abused in reality.

Participants generally agreed that the laws and excerpts which explicitly and clearly protected a right to use strong encryption were human rights respecting and that very strong safeguards were needed on those compelling decryption.

Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways (3 paragraphs):

- Strong encryption by default should be the norm
- Any restrictions on the use or deployment of strong encryption should be very limited, targeted, the law should be clear, there should be due process, and strong safeguards against abuse
- The ramifications of encryption workarounds, including decryption and use of hacking in particular, on human rights are still unclear and the debate on this continues. The debate on encryption workarounds needs to be conducted in an inclusive and transparent manner so that relevant policies are human rights respecting

<u>Gender Reporting</u>

Estimate the overall number of the participants present at the session:

40

Estimate the overall number of women present at the session:

20

To what extent did the session discuss gender equality and/or women's empowerment?

The session did not focus on women in particular but as it focused on encryption and the role of encryption as an enabler of human rights, it can be said that it was referred to in so far as encryption is an enabler of women's empowerment and rights and thus creates safe spaces for women to communicate.

If the session addressed issues related to gender equality and/or women's empowerment, please provide a brief summary of the discussion:

N/A