Session report Open Forum 40 THE NEW CORPORATE DIGITAL RESPONSIBILITY: DUTIES OF CARE AND THE INTERNET OF THINGS

On behalf of the Dutch National Cyber Security Council (CSR), the Dutch Ministry of Justice and Security hosted an Open Forum on the topic of duties to care in ICT with a focus on Internet of Things (IoT). This Open Forum was held in the form of an open discussion between all present, allowing to "pick the brains" of the attendees, with a few pre-selected participants International Chamber of Commerce (ICC), Dynamic Coalition Internet of Things (DC IoT), Best Practice Forum Cyber Security (BPF CS) and Australian Computer Science (ACS) who were invited to make an intervention as "representative" of the different stakeholder communities within the Internet Governance Forum (IGF).

Cyber Security Council introduction

In April 2017 the CSR, an independent, high-level, public-private-academic, advisory body to the Dutch Cabinet, published the cyber security guide for businesses: 'Every business has duties of care in the field of cybersecurity'. It presents a strong case why companies using ICT have duties of care, for itself, its customers and its environment, based on already existing rules and regulations. The guide points companies towards actions that ensure viable cyber security measures and solutions. It is important to share best practices at the IGF. Other states can transform this cyber security guide to the judicial framework of their state and make a checklist as well.

NL IGF

The CSR and the participants of the preparatory discussion at the NLIGF agreed there is a need for global harmonisation of these duties of care. Invitees were sent a few questions in order to prepare for the Open Forum. This led to a more focused discussion.

In situ poll

In general the conclusion is justified that there is a need for (the harmonisation of) duties of care in ICTs and that these can only be reached through multistakeholder processes. **The IGF is the right venue to facilitate process on a complex and critical Internet issue like duties of care. Several strong pleas were made to try and do so, e.g. involving National Regional IGF's (NRI's).** It is justified to conclude that the CSR document was very well received on this global stage.

Industry

Duties of care so far are mostly self-regulatory industry measures, e.g. the technical measures that make the Internet work and measures service providers take to protect customers. The question that should have been asked is: what duties of care can be harmonized globally? This includes crossing socio-political differences, a sustainable economic model and allowing for permissionless innovation. It is important to find the right balance between all these constellations.

Dynamic Coalition on IoT (DC IoT)

There is a role for all stakeholders (industry, service providers, consumers, civil society and government) in this debate as not one can solve this alone, with a specific responsibility for industry to produce safe products. **What better place than the IGF to bring all stakeholders together and discuss potential ways forward. In the DC IoT the participants share good practices from a multistakeholder perspective.**

Consumer protection

Consumer protection is absent in the CSR cyber security guide for businesses. More in general consumer protection agencies are absent in the discussion of duties of care because they have not yet arrived in the new digital era. The view was shared the topic should be broadened to forms of regulation or oversight on AI, neuro networks, autonomously working software and data and who owns data. It was pointed out later that at the European level organisations like the European Consumer Association (BEUC)[1] and ANEC (the European consumer voice in standardisation) are active in this field, but may need to be introduced to this specific line of work within the IGF.

The Best Practise Forum on Cyber Security (BPF CS)

The Best Practice Forum on Cyber Security is looking into future work. One topic is the development of norms. The CSR cyber security guide for businesses translates responsible behaviours and expectations of participants within cyberspace and participants that may deploy software or may utilize software to deliver services in a very practical way. To be successful it has to be made very practical and clear what is expected of every stakeholder in order to be a responsible stakeholder within that environment. **It is an approach we are looking at for 2018. Duties of care is one of several potential topics of the BPF in 2018, should the MAG decide it should continue.**

Global Forum of Incident Response and Security Teams (FIRST)

From a Computer Security Incident Response Team (CSIRT) point of view duties of care could be looked at how harm can be minimized, just like the goal of FIRST members is to minimize the effects of incidents.

Technical community

There's a need for focus and that is on IoT. There is a need to define duties of care and what we try to achieve. The different judicial systems must be taken into account. It's important to recognise what already exists. Several participants pointed to existing initiatives that need to be included in this broader discussion.

General discussion

An important point made, was that the CSR cyber security guide for businesses was professionally supported. **That will make it hard to duplicate elsewhere, but is seen as a potential and interesting exercise for NRIs to try and collect locally available data to share globally and contact institutions**

[1] **The European Consumer Organisation** (BEUC, stands for French "Bureau Européen des Unions de Consommateurs") is an umbrella consumers' group, it brings together 42 European consumer organisations from 31 countries.

that can take on the CSR function in their respective constituencies. The BPF CS would like to contribute to this and is willing to share the information in the BPF CS.

Part of the discussion focussed on the analogy between healthcare and digital health. Yes, there is a need for better trained end users, but in the end products need to be made available that even the most naïve can work safely with. There was a rough consensus on this topic.

An important question in the discussion about duties of care is 'who is the owner of data?' Transparency about the use of data is important. Only when it is made clear who owns the data, it is possible to say something about this in a legal way.

Conclusion

Many agreed that the the CSR cyber security guide for businesses presented in this session and shared as a good practice is one that should be disseminated across the world as a way to drive this discussion forward. There was 100% consensus on the need to bring the topic of duties of care in ICTs further, with a rough consensus whether the IGF could facilitate some parts of this discussion. If it does, the IGF should make it as precise and prioritized as possible with a predefined sort of desired outcome that would make it more feasible for several stakeholders to participate in the process. This is a prerequisite in order to have a chance at success. It was pointed out during the session that there are existing initiatives that should not be duplicated, but learned from and/or could be connected to future IGF work. Some saw a role for NRIs, to make data available, both ways.

Duties of care has been noted as one of the potential topics of the BPF Cyber security next year.