UN Human Rights B-Tech's IGF panel
"Upholding Rights in the State-Business Nexus: C19 and beyond"

Introduction

On 6 November 2020, B-Tech hosted an open forum at the Internet Governance Forum to explore how human rights can be protected when States cooperate with technology companies, departing from the developments in response to the Covid-19 pandemic. The B-Tech Project seeks to provide authoritative guidance and resources to enhance the quality of implementation of the United Nations Guiding Principles on Business and Human rights with respect to a selected number of strategic focus areas in the technology space.

The panel set out to explore what are the challenges of upholding human rights in the state-business nexus as set out in the UN Guiding Principles. The panel explored an aspect of the smart mix of measures as included in the UNGPs, the state-business nexus. Recognizing that when States cooperate with, when they procure from or partner with technology companies, States need to take their own role in incentivizing those companies to respect human rights but also make sure that they meet their human rights obligations as they do so. Companies developing new technology products and solutions to fight the spread of the virus, coupled with the rapid and extraordinary government requests for access to user data raises major human rights concerns and questions:

- How do we protect privacy rights while using technology to address legitimate public health and safety issues?
- How can we prevent that governments use data about their citizens for nefarious purposes? How do we manage the risk of discriminatory access to information and public health outcomes, or social stigmatization?
- What is an appropriate timing for rolling back special measures with elevated human rights risks?
- How does user data need to be governed to uphold purpose limitation (e.g. public health)?

Gary Davis, Global Director of Privacy and Law Enforcement Requests at Apple, described how the global outbreak of Covid-19 in early 2020 had abruptly resulted in increased outreach of governments to the company. This culminated in the decision of Google and Apple to pursue a joint effort to enable the use of Bluetooth technology to help governments and health agencies reduce the spread of the virus, with user privacy and security central to the design. In his comment, Gary Davis emphasized the following:

- *Strong privacy and trust as a pre-condition for broad adoption:*

In early conversations with public health agencies, some proposals for contact tracing solutions would, if implemented, undermine privacy. But strong privacy and data protection safeguards are critical to ensure user trust and uptake. This in turn increases the efficacy of tech-based solutions in fighting the pandemic.

- *Privacy-oriented principles and design of the technology:*

The Apple and Google Exposure Notification technology was designed to gather the minimum amount of data necessary to ensure effective contact-tracing through decentralized systems, with users needing to take pro-active steps to turn the tracing app on, such that there is no sharing of users' location data, and also to ensure user make the active decision about reporting a diagnosis, and that users' identities are protected and solutions remain interoperable.

- *Access has been an important consideration:*

The company sees one benefit of their approach as enabling governments with less technology expertise to provide contact tracing solutions. This is also one driver for Exposure Notification Express which allows governments to deploy contact tracing without having to build their own App.

Stephanie Hankey, Co-Founder and Executive Director of Tactical Tech, outlined the strong necessity to widen the frame of reference when speaking about human rights impacts of technology solutions in the state-business nexus. She highlighted these key aspects:

- *The need for more clarity, principles, norms, laws about States governing technological use and data:*

The pervasiveness of the collection and analysis of behavioural data in contemporary society raises important governance questions: a lot of tech in the response to Covid-19 has been modelled to understand the risks as well as to predict users' behaviour, and assist in enforcing lock downs. A large share of this technology, e.g. wearable trackers, was used to see if people have left their home or not, and to look at behaviours overall. Hankey claimed that while many technologies feel "new", they have been used for a long time, such as data from mobile phones, credit cards, CCTV. The way in which this data is used is not always successful for serving the purpose it was supposed to fulfill, but nevertheless results in an unprecedented synthesis of private and public data, and raises a range of questions from a human rights perspective, including about consent.

- *Looking beyond the big-tech players to who else government is working with:*

While the public discourse often focusses on the role of a set dominant multinational companies in technology governance, there is a need to balance out the focus of attention from Big Tech players to encompass also the many mid-size and smaller players. These smaller players have been equally engaged by States during the pandemic, and some of which have dubious human rights records.

- *The concern with normalization of States gathering and using behavioral data for, in principle, public good and to address crises:*

Hankey criticized the normalization of the idea that States need citizens' behavioural data. Sh highlighted the adverse impacts that the same technology used for responding to the pandemic when used to track human rights defenders and journalists.

- *Challenges of governments playing a stronger governance or implementer role - Computing power and engineering power is not in States, but in companies:*

Hankey outlined how society needs to define more clearly what is the actual problem it wants to address, who controls and holds the assets and which role human rights and rightsholders play, including how they can have a say in decision-making.

Phil Dawson, Public Policy Lead of Element AI, spoke about his experiences around conceptualizing "smart" cities and data-driven management of municipalities in rights-respecting ways and associated risks in the grey area of who is responsible for what in public-private-partnerships. Phil Dawson's contribution focused on the following elements:

- *The challenge of appropriate oversight mechanisms:*

Dawson emphasized the need for institution building around the governance of public-private initiatives. This should include channels for meaningful civic engagement and participation in project decisions that impact human rights, including mechanisms for contesting decisions. Dawson noted that national and local governments should be cautious about relinquishing the ownership of digital infrastructures developed through public-private partnerships, which can lead to an abdication of public interest governance, oversight and accountability.

- *Digital infrastructure and civic tech governance - enable public oversight of digital tech (own engagement, own grievances, own governance):*

Dawson highlighted the importance of conducting human rights impact assessments to better understand project risks and how these may be mitigated through appropriate governance structures, particularly where the State is partnering with the private sector to carry out such projects. Such assessments should be based on the UN Guiding Principles on Business and Human Rights and the Universal Declaration of Human Rights, and ensure that the local government applies human rights in the local context, for instance, as articulated through documents such as the Declaration of Cities Coalition for Digital Rights.

- *The role of contracting and accountability structures:*

In the absence of new data governance structures, an effective way to promote respect for human rights in public-private projects in cities can be to translate digital rights into precise contractual obligations that urban developers and their partners can be made to comply with. This, of course, requires that State actors invest time and resources into the identification of potential risks to human rights posed by a particular project, and should therefore be clearly stated *a priori* in requests for proposals.

John Howell, Director for Human Rights Scrutiny at the Australian Human Rights Commission, reported from his experience consulting with government and business on technology and human rights, and representing rightsholders' interest when the government uses technology that impacts its citizens. John Howell brought forward the following points:

- *Role of NHRI to flag rights-focus vs. ethics perspective:*

Many recent initiatives to ensure new technologies are used for good have focused on ethical frameworks. While it is good to have ethics, the strengthened focus on rights provides the precision in content that ethics might lack in values relativism. The normative weight of human rights was highlighted in the Commission's work on automated decision-making. Recent deployments of AI by government in an Australian context had not fully considered human rights impacts – these included a system of automated social security debt recovery ('Robodebt') and proposed Facial Recognition legislation with automatic enrollment; creation of a national database of images and authorizing real-time identification by law enforcement and national security agencies. Howell emphasized that human rights embody fundamental values that can be applied in such particular context of automation, and allow for robust and clear assessment of the impact and proportionality of measures such as these.

- *Proposal of AI Safety Commissioner: Internal capacity and coherence with subject matter expertise:*

John Howell championed the idea of an AI safety commissioner to protect and promote human rights as a fundamental value of particular concern, to build capacity in government and industry in relation to promoting and protecting rights when designing, procuring and deploying AI systems, and also to help build trust in the community. In the context of the government-business nexus, the proposed AI Safety Commissioner could serve as a leadership body overseeing the impact of state-business cooperation in tech on people. This leadership body could frame the thinking how AI could be regulated and respond to the need for government and industry using these tools to get a better understanding on how to deploy technology tools in the state-business nexus in a human rights compliant manner. The commissioner could build such expertise and provide ongoing support to regulators for subject matter and guidance for governments and cities.

Outlook

In the upcoming month, B-Tech will further deepen its work on the state-business nexus and build on the insights emerging from this panel, working with a range of actors from civil society, business, States, and other experts.

If you would like to notify the B-Tech Project team of, or invite us to, relevant events, or propose organizing an event with us, please contact B-techproject@ohchr.org.