Transcript of Webinar #2

# Business and Human Rights in the Digital Environment

# 01 Welcome

Hi again, and welcome to the second of this four-part webinar series on business and human rights in the digital environment. My name is Richard Wingfield, Legal Officer at Global Partners Digital.

# 02 Agenda

In the first webinar, we looked at the field of business and human rights broadly, with a focus on the UN Guiding Principles on Business and Human Rights. In this webinar, we will look at how this framework applies to the digital environment.

We will look at how the state’s duty to protect, the companies’ responsibility to respect, and the adoption of grievance and remedies mechanisms operate in the digital environment. We will also look at some examples of good and not so good practices under each of the three pillars.

# 03 Cambridge Analytica

In 2014, thousands of people completed an online quiz on Facebook. In doing so, they unknowingly shared their personal data, and their friends’ personal data, with Cambridge Analytica, a company that worked for President Trump’s 2016 election campaign.

So, what happened and what was the impact on human rights? Well, Cambridge Analytica is a research firm, which partnered with a UK-based academic, Aleksandr Kogan, who was using Facebook data for research purposes. Quizzes were sent to around 300,000 people in the US.

To take the survey, you had to log into Facebook, which gave Kogan access to your profile, including your birth date, location and, most importantly, your Facebook likes. Kogan combined the quiz results with your Facebook data to develop a psychometric model, a sort of personality profile. He then combined this with voter records and sent them to Cambridge Analytica.

But the test also took the personal data of your Facebook friends and compiled similar profiles of them. In just months, 270,000 people had taken Kogan’s survey, and the data of up to 87 million friends was also harvested – close to one quarter of all US Facebook users.

So, was this a data breach? Facebook says no – no passwords were stolen, and no systems were infiltrated. But Mark Zuckerberg has said it was a breach of trust between Facebook and its users. And the right to privacy of 87 million people was affected, as they weren’t in control of the use of their personal data.

Should Facebook do more in terms of human rights?

# 04 Recap from Previous Webinar

The Facebook-Cambridge Analytica case involved a series of different actors, including companies, government and academic institution who may have potential responsibility for adverse human rights impacts. Before looking at those potential responsibilities it is important to note three things when applying the business and human rights framework to the digital environment:

First, governments have the duty to respect, protect, promote and fulfil human rights. That duty includes ensuring that national laws, regulations and policies are consistent with international human rights laws and standards, including on human rights which are particularly relevant to the digital environment, such as freedom of expression and privacy.

Secondly, tech companies have the responsibility to respect the rights to freedom of expression and privacy of their users. To do so, they should comply with all applicable laws and respect internationally recognized human rights, wherever they operate. If national laws, regulations and policies do not conform to international standards, tech companies should avoid, minimize, or otherwise address the adverse impact of government demands, laws, or regulations, and seek ways to honor the principles of internationally recognized human rights to the greatest extent possible.

Thirdly, the government should ensure that wherever adverse human rights impacts occur, individuals have access to judicial and non-judicial grievance and remedial mechanisms. We will look at some examples of claims against tech companies, and tech companies’ grievances mechanisms, as a way to address potential adverse human rights impacts.

# 05 Introduction

Technology companies have not always been the main focus in the business and human rights field. However, they have started to gain greater attention due to recent high-profile cases, such as the Cambridge Analytica scandal.

When the UN Guiding Principles were being developed, the main sectors that grabbed attention and discussions were companies that operate through extended supply chains and extractive companies. Tech companies were usually considered only narrowly in the context of censorship and surveillance.

In fact, during that period, and due to the Occupy movement and the Arab Spring, tech companies, and the platforms they provided, were seen as an enabler for democratic activism. So, tech companies were mostly seen as enablers of human rights, rather than threats to it.

In recent years, however, we have seen how technology tools have been used for mass surveillance and to influence political elections. We have also observed network disruptions and data breaches.

In that time, freedom of expression and privacy have risen to the top as prominent issues in the ICT industry. These topics will be explored further in the final two webinars delivered by the Open Technology Institute.

# 06 Introduction

The impacts of tech companies are particularly felt when it comes to the rights to freedom of expression and privacy, and there are initiatives such as the Global Network Initiative focused on protecting and advancing those rights in the sector.

But their operations have implications for a much wider set of rights. The UN Human Rights Council has endorsed a broad approach to human rights and the internet through a series of resolutions affirming “the same rights that people have offline must also be protected online”.

# 07 Pillar 1: State Duty to Protect

Let’s take a look at each of the three pillars under the UN Guiding Principles.

The foundational principles of Pillar 1 says that states ‘must protect against human rights abuses by third parties (including business enterprises) within their territory and/or jurisdiction’.

A key question is how to apply this principle to tech companies given that they are often global and not based in the jurisdiction of the state that may try to protect human rights abuses. While the UN Guiding Principles say that states are not generally required to regulate the extraterritorial activities of businesses, they also recognize that that states are not generally prohibited from doing so, provided there is a recognized jurisdictional basis. The UN Guiding Principles recognize that there may be strong policy reasons for states to be clear about the expectations of businesses abroad.

When it comes to operational principles, in the previous webinar we saw that one tool that governments have to protect human rights in the digital environment is legislation and regulation. When passing new legislation or regulations, it is essential that any legislative or regulatory frameworks developed which apply to online platforms or communications services, or other new technologies, facilitate, rather than undermine the enjoyment of human rights.

There are a number of cases where despite trying to prevent the potential negative consequences of technologies through legislation, governments have ended up putting other human rights at risk. For example, the right to erasure, or the “right to be forgotten” that is now formalized in the EU’s General Data Protection Regulation, has the potential to address legitimate privacy concerns, but also has potential impacts upon the rights to freedom of expression and access to information.

# 08 National Action Plans

Another way that states can fulfil their obligations under the first pillar is through National Action Plans on Business and Human Rights, or NAPs, and they should include digital issues. However, not much has been done so far. Most NAPs’ commitments do not necessarily relate to specific forms of protection, responsibility and remedies, but just lay the ground for potential developments on specific issues related to ICTs. For example:

The Swedish government highlight in its NAP that internet freedom and privacy are among the great global issues of the future. It states that it is fundamental for Sweden that the human rights that apply offline also apply online, adding that as a result of a Swedish initiative, the OECD Guidelines for Multinational Enterprises now call on companies to support human rights on the internet. Yet apart from these important developments the Swedish NAP doesn’t highlight any action points or future development in the field.

Similarly to Sweden, the Irish NAP highlights past actions such as providing a fourfold increase in the funding for the work of the Data Protection Commission in recent years; and the UK NAP highlights that it has strengthened international rules relating to digital surveillance, including leading work in the Wassenaar Arrangement to adopt new controls on specific technologies of concern.

The Netherlands undertook a Sector Risk Analysis in 2014 which identified the electronics sector as among those with the greatest risk of adverse human rights impacts. The government has committed to negotiating voluntary corporate social responsibility agreements that focus on transparency, dialogue with stakeholders, and monitoring of agreements with those sectors.

Other countries have developed action points, in particular, the Polish government in its NAP has committed to draft a regulation to counteract restrictions on the freedom of speech. And the Finnish NAP has proposed to create a roundtable discussion on how to ensure the protection of privacy in Finland with the government agencies, ICT companies and civil society.

# 09 Pillar 2: The Corporate Responsibility to Respect

The second Pillar of the UN Guiding Principles says that companies are obliged to respect national laws in the jurisdictions where they operate. But their responsibility to respect rights exists over and above compliance with national laws and regulations which protect human rights.

Beyond national legislation. What should we expect from companies? Well, there are a few things:

* Companies should make an explicit statement affirming their commitment to freedom of expression and privacy as human rights and to demonstrate how these commitments are institutionalized within the company.
* Companies should disclose clear evidence of: senior-level oversight over freedom of expression and privacy, and employee training and whistleblower programs addressing these issues.
* Companies should undertake human rights due diligence and impact assessments to identify the impacts of the company’s products, services, and business operations on freedom of expression and privacy.

# 10 Pillar 2: The Corporate Responsibility to Respect

The starting point for company implementation of the UN Guiding Principles is the adoption of a human rights policy commitment.

A small but increasing number of ICT companies have adopted comprehensive human rights policies that embrace and are explicitly aligned with the UN Guiding Principles. However, implementation of human rights policies and procedures in the sector reflects the tendency of companies to respond only to those issues that have triggered serious reputational risk. The Business and Human Rights Resource Centre maintains a list of company policy statements that reflects this tendency.

A number of civil society organizations have argued that companies’ policy commitments usually pick and choose which issues to frame as part of their human rights commitments. But, there are some companies, such as Microsoft which have developed a broader human rights policy that explicitly includes all human rights as per the Guiding Principles.

# 11 Due Diligence

Identifying risks and implementing mitigation strategies, particularly when those strategies have serious impact on revenue, requires support from across the company, particularly at the highest level.

Another way to comply with these obligations is through transparency reporting. In 2010, Google became the first company to report on government requests, followed by Twitter in 2012. By 2014, more than 40 companies around the world released transparency reports, and the number continues to grow.

We’ll be looking at this subject in the final two webinars and the in-person workshop.

# 12 Pillar 3: Remedies

Transparency and commitment from across the company is, however, not sufficient. There should also be some form of grievance and remedies mechanisms, where the company recognizes that their actions have led to adverse human rights impacts, which leads us to the third pillar.

The UNGPs recognize the right to an effective remedy when companies are involved in human rights abuses. As we have seen in the previous webinar this is a responsibility of both states and companies.

In terms of the state’s commitments, they should help to avoid barriers to access judicial remedies. And this obligation may include training of judges on issues related to technology.

From a non-judicial point of view, governments can support the role of independent institutions such as National Human Rights Institutions, or ombudsperson’s offices that may have enforcement powers, to understand the sector.

# 13 State based

Despite the increasing adoption of the Guiding Principles by tech companies, access to effective remedy is less established in the ICT sector compared to other industries that have faced serious human rights scrutiny, such as the extractive industry and manufacturing.

In those sectors, human rights defenders and civil society are pressing companies to ensure effective grievance mechanisms. In the ICT sector, getting companies to establish any sort of grievance mechanisms framed explicitly in line with the UN Guiding Principles has proven challenging.

However, there have been a number of legal cases brought by individuals against tech companies in different jurisdictions. For example, the case of Xiaoning et al. vs. Yahoo. This lawsuit filed in 2007 followed Yahoo’s cooperation with the Chinese government’s requests for user data that led to the imprisonment and abuse of two dissidents. The case resulted in a settlement and the creation of a fund to support Chinese activists, although the management of that fund has recently come under scrutiny.

In addition, data protection authorities have fined tech companies a number of times in different jurisdictions, particularly in the European Union. Yahoo! UK Services Limited, based in London, was fined £250,000 by the UK Information Commissioner’s Office after their computer network was compromised as the result of a cyberattack in November 2014. And Facebook was fined 1.2 million euros ($1.4 million) by the Spanish Data Protection Agency for allegedly collecting personal information from users in Spain that could then be used for advertising in 2017.

# 14 Non-state based

From a company’s perspective, the third pillar means that the company should have grievance and remedial mechanisms to address users’ freedom of expression and privacy concerns.

Ranking Digital Rights has been measuring different elements of the grievance and remedial mechanisms adopted by companies, in particular looking at the following elements:

* Does the company clearly disclose its processes for receiving complaints?
* Does the company clearly disclose that its process includes complaints related to freedom of expression and privacy?
* Does the company clearly disclose its process for responding to complaints?
* Does the company report on the number of complaints received related to freedom of expression and privacy?
* Does the company provide clear evidence that it is responding to complaints?

# 15 Company grievance mechanisms

According to the results of RDR’s research, the grievance mechanisms and remedial processes provided by comapanies should be more prominently available to users.

Companies should more clearly indicate that they accept concerns related to potential or actual violations of freedom of expression and privacy as part of these processes.

Beyond this, disclosure relating to how complaints are processed, along with reporting on complaints and outcomes, would help ensure that the mechanisms follow strong procedural principles, and that the company takes its grievance and remedy mechanisms seriously.

# 16 Next

We hope that you have obtained a good overview of business and human rights and the digital environment.

In the next two webinars, the Open Technology Institute will look in more detail at two priority issues: privacy and freedom of expression.