Transcript of Webinar #3

# Key Priority Issue: Privacy

# 01

Hi again. Welcome to the third webinar of this four-part webinar series on business and human rights in the digital environment. My name is Spandana Singh at New America’s Open Technology Institute.

# 02

In the previous webinars, our partners at GPD introduced the field of business and human rights, including the primary principles and framework that apply to the digital environment. In this webinar, we aim to provide a foundational overview of one of the key priority issues in the space of business and human rights in the digital space -- privacy. This will include discussions of privacy from companies, as well as from governments, and it will also include a discussion of best practice frameworks for understanding and assessing privacy in the digital age.

# 03

As technology has developed it has opened up a number of opportunities for individual expression and coordination including for human rights activists and defenders. However, it has also made individuals susceptible to surveillance and vulnerabilities which threaten their privacy and security.

Privacy can be defined as “the right to be free from unwarranted intrusion and to keep certain matters from public view.” Privacy has long been recognized in international law, but the combination of rapidly evolving digital technologies, the expansive applications of these technologies and the aggressive collection of personal information by states and corporations has eroded these privacy rights and undermined their enforcement.

International frameworks such as the The International Covenant on Civil and Political Rights recognizes the right to privacy, stating that “no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honor and reputation” It further states that “everyone has the right to the protection of the law against such interference or attacks.”

Other international accords and agreements also discuss the right to privacy. These include the OECD’s set of “Core Privacy Principles,” the Council of Europe’s “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,” APEC’s “Privacy Framework” and the EU General Data Protection Regulation (GDPR). The UNGP’s, which were discussed in the previous webinars also provide guidance for how companies should integrate respect for human rights-- as outlined in frameworks such as the UDHR and ICCPR-- into their business practices.

# 04

As access to private information online has grown, with and without consent, security has also emerged as a key concern. Protecting data security means allowing individuals to control who has access to their data, how the information is collected, used and stored, and implementing safeguards to protect against data breaches through unwarranted access methods such as hacking.

# 05

The GNI Principles also emphasize the need for privacy, calling for companies to employ protections that respect the personal information and privacy rights of their users, particularly when confronted with government demands that aim to unjustly compromise privacy.

# 06

When we think about privacy in the digital era, we need to distinguish between privacy from companies and privacy from governments. Companies regularly collect and use our data to target individuals with specific advertisements and otherwise tailor their individual experiences. Governments also regularly gather data through various programs including surveillance programs and can use this data in a criminal prosecution or misuse it to stifle the free speech of political opponents. The risks of an intrusion into your privacy and the legal frameworks that apply to both of these streams are very different. For example, although the ICCPR applies to both privacy from companies and privacy from the government, the EU’s new GDPR framework only applies to companies. In the United States, we do not have a data privacy regime yet, and the 4th Amendment says nothing about what a company can and cannot do, but rather only applies to the government and protects against unreasonable searches and seizures.

# 07

Over the past few years, we’ve seen just how integral strong privacy and security

protections are for users, companies and governments alike. The Cambridge Analytica scandal, for example, saw political data firm Cambridge Analytica gain access to the private information of over 50 million Facebook users, impacting political operations and elections in countries across the world including Kenya, Colombia, Indonesia and Albania. In addition, the Yahoo scandal in which 3 billion user accounts were compromised have highlighted just how vulnerable user data is to being accessed by third parties through hacks as well as through weakly enforced corporate policies. On the other hand, companies can play a critical role in protecting user security and privacy. For example, in the Apple vs. FBI case, Apple took a strong stand in favor of users’ security and privacy when the FBI asked Apple to design new software that would enable the agency to unlock an iPhone, they had recovered from one of the shooters in the December 2015 terrorist attack in San Bernardino, California. This case highlights the important role companies can play in protecting and managing user privacy from governments as well.

# 08

As technology adoption increases dramatically, whether it is through use of connected consumer devices or engagement with online services or platforms, companies have become responsible for dramatically larger troves of their users’ data. They have also begun to collect new types of data, which pose particular risks in cases of data breach, like biometric data, location data, communication data and audio and video recordings. This information, combined with traditional sources of data, can paint a highly detailed portrait of a user’s life.

This raises a variety of issues surrounding the collection of data, the use of data, the retention of data and the security of data. In order to protect their users’ data privacy and security while maintaining consumer trust, companies need to develop clear policies around each of these issues and then ensure that those policies are effectively communicated to all users of their products or services.

# 09

Best practices around data collection are two pronged:

First, in order to protect user privacy and security, companies should minimize the amount of data they collect. Ideally, companies would not collect information beyond what is necessary to use a product or service. This data minimization protects the privacy of users by not over-collecting, for example requiring address book or microphone access to play a mobile game, or a platform requiring constant access to a user’s photo library. Any information collected by a company is vulnerable to accidental breach or hacking and provides more opportunities for a user’s privacy to be violated.

Second, it is a best practice to make it clear to consumers what information is being collected and when. This can be done through tools like a terms of service, which could also be called “community guidelines,” “terms of use,” or “terms and conditions.” Users could also be given the opportunity to affirmatively authorize collection (through a request or notification) and using tools like a light identifying that a camera is recording or some other indication that information is being actively collected at that time, are important steps toward protecting users’ privacy and security.

# 10 N/A

# 11

Best practices for data use involve notifying consumers about the ways in which their data is used, and the parties or services that use that data. For example, if data is going to be used for any purpose other than those required by the device or service, like direct marketing, this is something that consumers should be notified about. Ideally, they will also have the option to opt out of this type of data use and control other settings. Similarly, if user data will be sold to or shared with any third parties, including government actors, it is a best practice that users be notified of the potential that their data may be shared and who with.

# 12 N/A

# 13

Best practices for data retention involve minimizing how long each type of user

information is retained and disclosure of those timelines. Companies should not be keeping information for much longer than is necessary, and should delete all user information when users terminate their account or remove service from a device. Similar to concerns about over-collection of user data posing security problems, retaining data for longer periods of time than necessary can pose greater risk of security breach or misuse of information by the company holding that information. Some governments have regulations that require organizations to retain information for a certain amount of time, which should also be clearly disclosed to users.

# 14 N/A

# 15

Data security practices are extremely important for all products and services that collect information about their consumers. With the amount of personal data that many companies gain through the use of their products there is an obligation to take steps to protect that data from accidental leaks or data breaches. Key security best practices include encrypting user data at rest and in transit, authentication processes requiring strong and customizable passphrases from all users, providing regular patches or security updates to protect users from bugs or threats, and some sort of vulnerability management program that allows for the reporting of vulnerabilities to the company maintaining the product. As well, these data security practices should be accompanied by a transparent process for notifying consumers if their data gets breached.

# 16 N/A

# 17

When developing or refining a company’s privacy and security best practices, it is helpful to look to existing evaluation systems for guidance. Depending on the company’s specific products and concerns, there are different tools that can be helpful.

For example, The Digital Standard, a collective effort led by Consumer Reports, Disconnect, Ranking Digital Rights, and The Cyber Independent Testing Lab, with assistance from Aspiration, is a set of individual tests that taken together form a methodology for evaluating the privacy and security impacts of a given piece of connected software or hardware – generally IoT products or the software they can use. It was created to define and reflect important consumer values that must be addressed in the development of software and hardware products. The Standard is underpinned by a set of guiding principles: electronics and software-based products should be secure, consumer information should be kept private, ownership rights of consumers should be maintained, and products should be designed to combat harassment and help protect freedom of expression. So far, the Digital Standard has been used to evaluate Smart TVs and payment apps and report the results to consumers, but the possibilities are endless.

Other organizations or collaborations of organizations have developed their own best practices guides or evaluation metrics that apply to specific types of companies or models.

* The Open Technology Institute’s GETTING INTERNET COMPANIES TO DO THE RIGHT THING “Do the Right Thing” report focused on the historical conditions required for companies to adopt three different security best practices: transparency Reporting, two-factor authentication, and transit encryption by default. These case studies can be useful to companies looking at when and how others in their industry chose to adopt security best practices.
* The GNI Principles provide direction and guidance to the ICT industry and its stakeholders in protecting and advancing the enjoyment of global human rights. They also stress the value of collaboration between the ICT industry, investors, civil society organizations, academics and other stakeholders.
* The Electronic Frontier Foundation’s “Who Has Your Back?” project provides annual evaluations of how internet platforms and services protect the rights of their users

# 18

The laws governing surveillance vary from country to country, and involve different safeguards to ensure that government surveillance does not unduly infringe on individual privacy. In addition, governments collect vast quantities of personal data on their citizens for other purposes, ranging from financial information collected for tax purposes to personnel information on government employees, to sensitive health information. The four categories of safeguards that we have discussed with regard to companies – collection, use, retention, and data security – are also applicable to government collection of personal information.

In the context of surveillance, at the targeting stage, rules in the American legal regime limit who may be targeted for surveillance, what prior review or approvals are required before a government may conduct surveillance, what standard must be demonstrated to initiate surveillance, and the purposes for which surveillance may be conducted. For example, under the U.S. Foreign Intelligence Surveillance Act (FISA), surveillance may only be conducted to seek “foreign intelligence information,” a broadly defined term, and depending on the target and nature of surveillance, certain prior approvals must be obtained from the FISA court. Robust safeguards are necessary to ensure that governments focus their collection efforts on legitimate targets.

Once information has been collected, additional rules – sometimes called minimization procedures – will limit how information may be used, the length of time information may be retained, and what safeguards must be applied to secure data. These safeguards are especially important to safeguard the privacy rights of individuals whose information is collected “incidentally,” because they were in communication with a target of surveillance.

# 19

Government law enforcement and intelligence agencies may seek or compel the assistance of internet and telecommunications companies to obtain access to communications data in connection with their investigations. If a company or organization collects and stores data, the likelihood of receiving such a government request is high. As a result, it is vital that these companies prepare for handling such requests, and that users hold these companies accountable when managing their data. Before responding to a government request, companies should ensure that it is authenticated and complies with applicable law – in other words that it is really coming from a legitimate government entity, and that entity is entitled under law to seek the data.

There are a number of best practices companies can implement and users can push for in order to ensure the process of engaging with and responding to legal requests for user data is transparent and respectful of human rights. The first best practice is to develop clear policies for processing and responding to government requests. This is a critical but challenging process and must involve consultations with legal counsel. Only a lawyer can help a company identify lawful requests and develop effective compliance mechanisms. Based on our conversations with companies, we have identified a few broad considerations for ensuring procedures and policies are transparent and efficient.

# 20

**Tracking Requests:** Companies should have a single, centralized process in place to

track and tag requests and their status.

**Classifying Requests:** Companies should have an established procedure including

trained staff for reviewing incoming requests, classifying them and ensuring their validity.

**Responding to Requests:** Companies should work with their legal counsel to develop a playbook for responding to requests before they receive them. This will prevent errors and promote greater safeguarding of privacy and security.

Providing User Notice: Government requests are increasingly accompanied by a gag order which prevents companies from informing the target user of the investigation. For requests without gag orders, companies must decide whether and under what circumstances they will provide notice to their users. For requests with gag orders, companies must decide whether to challenge the other and/or inform users after the gag order has been lifted. Companies will also need to identify processes for contacting users.

**Keeping Data Secure:** Information about law enforcement and intelligence requests is sensitive information in itself. In order to keep this information secure, companies should carefully consider how this data is maintained and who has access to it.

**Challenging Requests:** Companies should have robust procedures in place that enable them to evaluate the validity and accuracy of requests, and challenge requests that do not comply with applicable law or that appear to infringe on privacy, human rights and security.

**Provide Public Overview of Policies and Procedures:** Users have the right to know how companies engage with such legal requests and how these requests can impact their data. As a result, companies should publicly disclose at least a high-level overview of their policies and procedures for responding to such requests.

# 21

Once a company has established these procedures, they should share at least a high

level overview of these guidelines publicly. This public version of their policies will serve as a resource for users, as it explains how companies engage with legal requests for their data and how these requests can impact individual users. This is also a resource for requesting agencies as it defines scope and viability of requests. These publicly posted policies should clearly explain:

1. What kinds of legal orders and mechanisms the company accepts and responds to? Depending on the company and country of operation(s), these could include court orders, MLATs, emergency disclosure requests, and search warrants;
2. The format in which requests must be made, such as in written form or through a specific company form; and
3. The scope of the request being made, which specifies the number of accounts or users, the product being targeted and so on.
4. The procedure the company follows for notifying users and any limitations that may exist to impacted users being notified

# 22

The second-best practice for responding to government requests for user data is for companies to publish regular and consistent transparency reports which provide quantitative and qualitative information on the scope and volume of government requests for user information they have received.

# 23

Transparency reporting is an extremely valuable practice that helps the public hold companies accountable as safeguards of user data and can be used to educate lawmakers on privacy issues. From a company perspective, transparency reports are a useful tool as they enable companies to communicate with their users and lawmakers about privacy and security, and are also a way of signaling company values and easing customers’ concerns about privacy intrusions. Many companies pressed the U.S. government for permission to disclose more statistical information about the extent of government data demands, to enable them to demonstrate that only a small percentage of their customers are actually affected.

OTI has published comprehensive toolkits and guides for companies which outline best practices for creating and expanding transparency reports, which we have shared links to in the supplementary materials. In addition, Ranking Digital Rights’ Corporate Accountability Index, which evaluates 24 of the world’s most powerful internet, mobile, and telecommunications companies, shows which companies are meeting these standards for transparency reporting and which companies are lagging behind. Links to the RDR Index are also provided in your supplementary materials.

# 24

Here are examples of the kinds of data that is shared in transparency reports on legal requests for user information. This is from Google’s transparency report on requests for user information which provides data from July 2009 to June 2018. This image highlights the number of requests the company has received for a particular reporting period. The data clearly shows a concerning trend of increasing number of requests worldwide.

# 25

This slide from the same Google report shows the percentage of requests in which the company produced some data to the requesting entity, and you can also see that the data disclosed can be sorted according to country.

# 26

Here is another example, this one from Microsoft’s latest transparency or Law

Enforcement Requests Report, which covers the period of January to June 2018. These data visualizations highlight the number of requests the company received globally, the number of accounts and users specified in the requests and how they responded, either by disclosing information, being unable to comply or rejecting the request.

# 27

Emerging technologies pose a whole host of new privacy and security challenges for both governments and private companies.

For example, the intelligence community is using artificial intelligence to help manage the exponential increase of data they are collecting. Computer analytics are used to read and understand the data, in order to free up humans for more specific tasks. Using AI, intelligence agencies are auditing routine functions that analysts, curators and collectors have manually done in the past. The National Geospatial-Intelligence Agency is using AI to sort large quantities of image data, helping the Agency to identify specific targets such as enemy safehouses and airfields. As in other types of data, this frees up humans who used to do this type of analysis manually to do more complex tasks that cannot be performed by a machine.

However, with the rising use of AI there is also a potential for unintended consequences with issues of privacy, transparency, safety, control, and bias. Artificial intelligence can exhibit dataset bias, association bias, interaction bias, automation bias, and confirmation bias. These can enter the system as the result of simple mistakes or oversight in data aggregation techniques, or due to the nature of machine learning algorithms which will perpetuate unknown biases in the data used to train the systems. There are movements to make ethical guides for AI, and it is a best practice for governments and other organizations to stress test their AI models and test for bias. Some of these best practices include making sure there are human analysts included in any AI data analysis to watch for potential bias, to ensure that key decisions are made by humans, and to balance the need for innovation with the obligation to benefit and safeguard society.

# 28

The Internet of Things provides a dramatically larger body of data for use by

third-parties, with 27.1 billion networked devices expected to be in use by 2021. Not only are connected home appliances and cars gathering troves of personal data, but technology that users carry in their pockets is now collecting biometric data, location data, images, audio, communications data, all sorts of user information that was, until-now, not easily available to companies and governments. Now these massive datasets provide opportunities for exploitation by nefarious actors, as well as general privacy violations through poor privacy and security practices. Much of this information is highly personal, and many users do not understand the potential consequences of their use of IoT devices.

# 29 Conclusion

In conclusion, as technologies develop and adapt, and as data becomes increasingly integral to the operations of these technologies, and society at large, threats to our privacy and security from both government agencies and companies are rapidly growing. As users, and members of civil society we need to be cognizant about how our data is being managed and used, and how we hold these actors accountable in their management of our data.

# 30 Next

Up next we will have our last webinar of this four-part series, which focuses on another key priority issue area – free expression online.