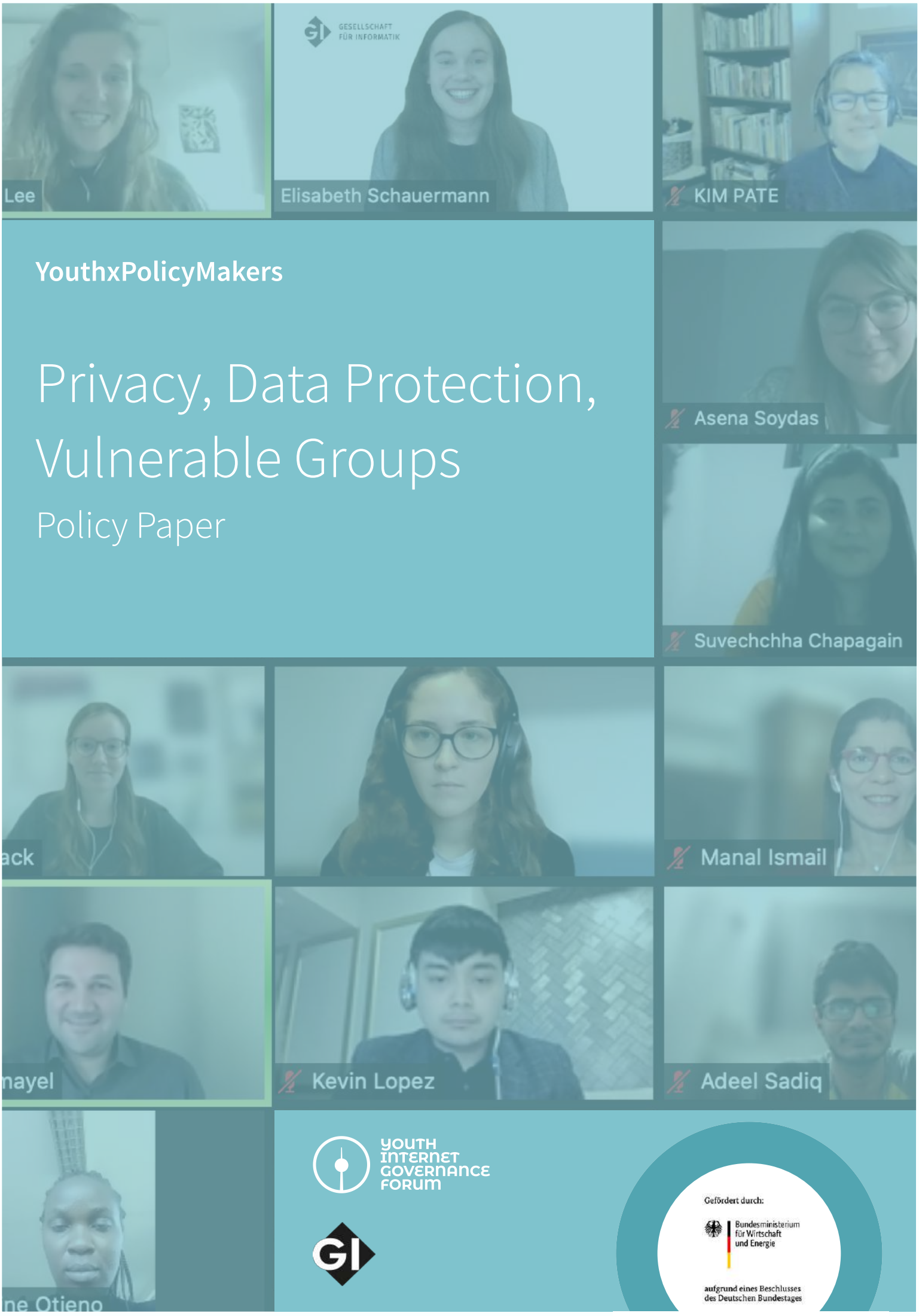


YouthxPolicyMakers

Privacy, Data Protection, Vulnerable Groups

Policy Paper

YOUTH INTERNET GOVERNANCE FORUM

GI

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Privacy, Data Protection and Vulnerable Groups

Mae Chew, Nicolas Fiumarelli, Sebastian Duda, Sofie Schönborn, Stella Teoh,

Mohammad A Jauhar, Ajay D M, Herman Ramos

Table of Contents

Introduction

2021 marks another year in which digital trust continues to decline. Unprecedented global changes like the COVID-19 pandemic have forced the majority of the globe's citizens deep into the embrace of the digital realm. However, this has come at a price. Now, most of us lack a comprehensive understanding of the technology and systems we rely heavily upon. We are increasingly exposed to new concepts that we have to digest and forced to make crucial decisions with incomplete information.

During the YouthxPolicyMakers 2021's fourth roundtable, selected ambassadors discussed the themes of privacy, security, and protection. This Policy Paper looks to summarise our view on the current state of affairs in these three focus areas, recap our takeaways from the workshop and roundtable stage before moving on to our demands.

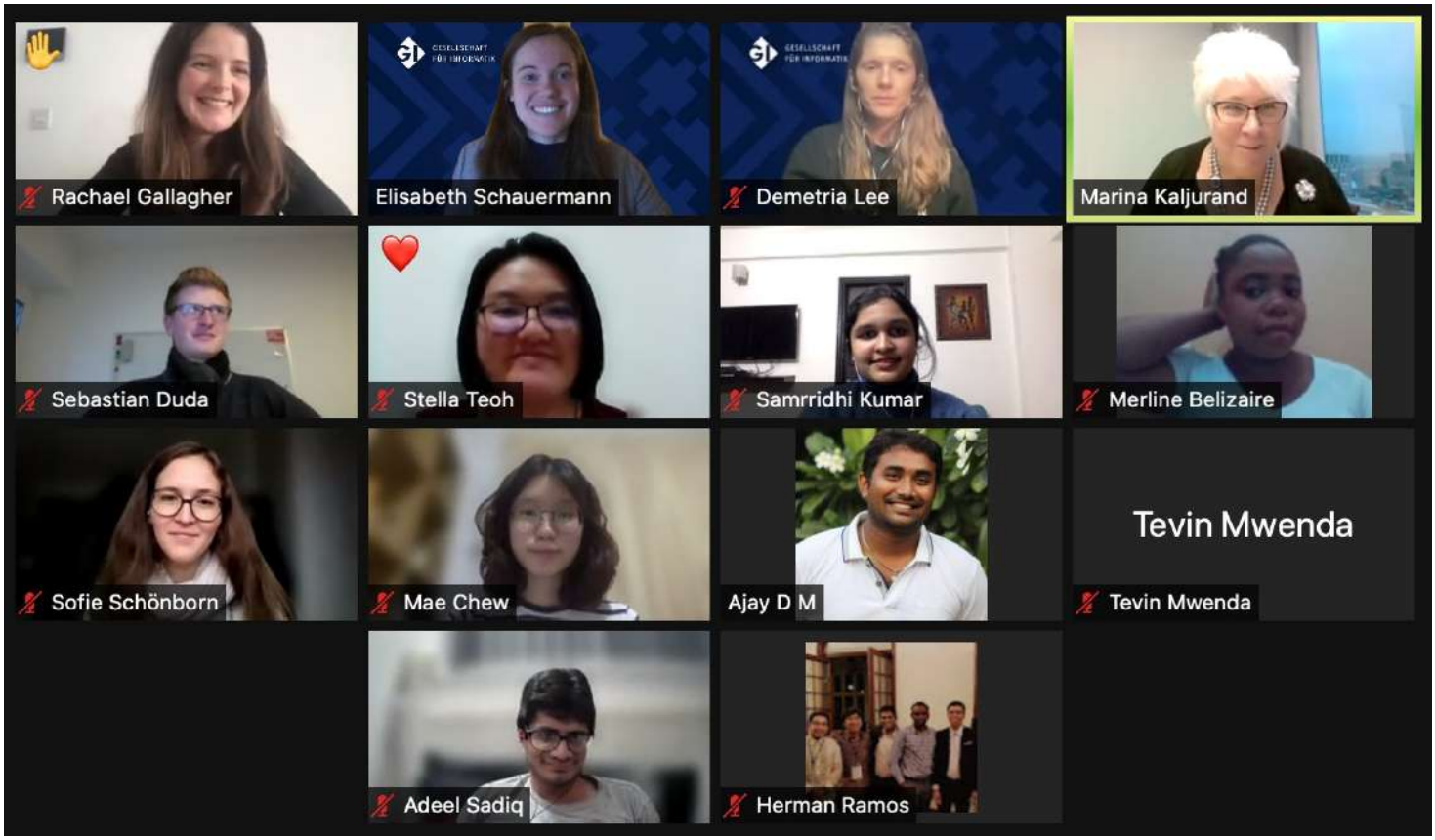
Current status of policy debates and processes

Privacy

Privacy is currently a hot topic in policy debates and discussions, and rightly so. Privacy has been one of the fundamental concepts found in all cultures across the world. The increasing use of technology around the turn of the millennium opened the door to broad data collection. Policymaking is slowly catching up with technological progress, but two major roadblocks are encountered. On the one hand, the infrastructure of the Internet is distributed across all jurisdictions. On the other hand, the institutions that currently own the data are unwilling to give their assets up. According to UNCTAD,[1] about 123 countries worldwide have put in place legislation to secure the protection of data and privacy. This rise can be attributed to the passing of the GDPR in Europe that acted as a catalyst that made the rest of the world aware of the need to safeguard peoples' data and privacy.

footnotes

1 Data Protection and Privacy Legislation Worldwide https://unctad.org/page/data-protection-and-privacy-legislation-worldwide



Security

Security in the digital space has been and will continue to be a matter of critical concern. Cyberspace is where crimes against citizens and wars against countries happen. This makes security a primary goal for every individual, business, and country to protect their sensitive data from various cyber-attacks.

Cybersecurity is an issue of global concern and curiosity, whether viewed in economic, humanitarian or national security terms. The cybersecurity market is predicted to reach 352.25 billion USD by 2026,[2] and cyber crimes shall cost the world around 10.5 trillion USD annually by 2025.[3] Poor infrastructure, lack of cyber security mechanisms, and prioritizing commercial interests over security constitute a significant problem worldwide, leaving businesses vulnerable to data breaches. State-sponsored threats with virtually unlimited computing power and finances are seen as a major threat to countries and global security. Hacktivists with an economic or political agenda—Script Kiddies—are seen as a major threat to the security of

footnotes

2 Cyber Security Market https://www.mordorintelligence.com/industry-reports/cyber-security-market

3 Special Report: Cyberwarfare In The C-Suite. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

internet users.

Recent instances where allegations have emerged against the interference of hackers/ hacktivists in elections threaten the democratic process established in countries. The lack of proper data protection policies, the security of citizens placed in the hands of a selected few companies and the ignorance of normal citizens of cybersecurity risks are critical contributors to the inflating concerns relating to cybersecurity.

Protection of vulnerable groups

Women, minorities, and individuals who experience intersecting forms of discrimination are often targets of rampant harassment and hate speech online. While Internet companies have made efforts to curb the spread of abuse on their networks, regulations are operationalized without regard for social contexts. For instance, the censorship of female nudity on Instagram and Facebook can be applied to images of indigenous cultural ceremonies, meaning that though the rules may provide the impression of being equitable, they retain the effect of marginalizing already marginalized groups.

Furthermore, the pandemic has magnified the lack of critical infrastructure to bridge the growing digital divide—of which indigenous communities, the elderly, women and other groups residing in rural or remote areas are on the wrong side. This structural reality perpetuates social, economic and political disparities, as digital illiteracy hinders their ability to access information, defend themselves against cyber threats and utilize applications that have the potential to transform their activities, opportunities and outcomes.

Lessons and positions resulting from the workshop stage

During the workshop stage, many ambassadors mentioned feeling exposed to privacy and security threats, particularly data and identity fraud. Coupled with the under-representation of certain groups, this results in a general lack of security for Internet users. When the discussion shifted to infrastructure, the general consensus was that poor governance in the digital world has real-world consequences (particularly when cyberattacks target critical infrastructure).

This ties in with the concept of digital identities functioning as extensions of our physical "real-world" identities. This was also later revisited during our roundtable with policy makers (on age verification). Most answers to the question about preventing problems revolved around raising awareness through education—digital literacy.

The last part of the discussion highlighted responsible stakeholders and challenges pertaining to these groups. Some acknowledged that due to different stakeholders' different interests, it was generally tough to adopt centralized solutions for identified problems as there were conflicts of interest. Another factor was the burdensome and lengthy process in policy and regulation. This is in stark contrast with the ever-changing technological environment, resulting in many instances where suitable legislation cannot be applied. The key takeaway from the workshop's discussion was that the Internet is a shared responsibility, where no one stakeholder is more responsible than the other.

Left, Rachael Gallagher, Privacy Policy Manager for Europe, the Middle East and Africa, Meta; right, Marina Kaljurand, Member of European Parliament, Estonia

Discussion with policy makers

In our roundtable, we had the chance to learn about and contrast perspectives from the public and private sectors. We discussed the need to acknowledge human rights online as applied offline (especially regarding Art. 51 of the UN Charter[4]) and were reminded not to forget

footnotes

4 Chapter VII: Article 51 — Charter of the United Nations — Repertory of Practice of United Nations Organs — Codification Division Publications

that humans should be the center of policy making. For this, civil society and NGOs are critical to hold other actors accountable and defend human rights.

Particularly after the COVID-19 pandemic, it has become clear that privacy, security, and protection of vulnerable groups are essential for our futures. Technical knowledge is rather low and uneven among policy makers, even though there have been many lessons from the pandemic. We discussed the need for digital topics to be higher on the political agenda and that the current window of opportunity for learning and increased action should be seized. We should now learn from successful cases, make information accessible and involve policymakers in debates on technology.

In all of this, we understand the importance of trust as a basis for collaboration between all stakeholders. Trust between the private sector, governments and consumers is important to jointly work on privacy, security and protection solutions.

Positions

PRIVACY*.* Privacy—not only in digital spaces—is an underlying right that facilitates other rights. For example, privacy is necessary to ensure a free press. Hence, we appeal to the policy makers to ensure privacy for people in any part of the world. This principle was consigned to paper in the UDHR §12. However, we identified several threats in the digital space that jeopardize privacy.

Governments have to protect their citizens. To do this, they have to choose between security and privacy. Often security is favored. One admired way to access data to investigate threats is to establish backdoors in cyber systems or weaken end-to-end encryption. Both, unfortunately, affect all devices and thus all citizens. The use of biometric information by governments,[5,6] and

footnotes

5 https://www.dw.com/en/new-german-id-cards-more-control-less-freedom/a-58088333
6 https://www.huffpost.com/entry/india-aadhuar-tech-companies_n_5b7ebc53e4b0729515109fd0

the private sector,[7,8] is a major risk to people's privacy. Biometric data like fingerprints or one's face cannot be changed. This can quickly result in severe threats in the physical world. To tackle data capitalism, it is necessary for regulators around the globe to advance local steps (GDPR, CCPA) and formulate and enforce privacy regulations on a global scale that can reestablish trust in these times of high privacy cynicism. Policymakers should encourage data reduction, data economy, privacy-by-design and security-by-design to avoid data abuse.

SECURITY. Cyberspace security is a critical priority for many as the well-being of individuals, businesses, and ultimately countries rely on it. Our position is that a security-by-design strategy should be incorporated in the development process of new technologies and applications to ensure compliance. We aspire for a multistakeholder approach for addressing concerns related to cybersecurity.

Governments should bring in policies and regulations that protect the interests and aspirations of citizens without affecting the rights while prioritizing national security. Ignoring security to avoid costs is a threat to the trust in technology and the Internet. Organizations must include security as their top priority with commercial interests. With the advancements in technologies like the Internet of Things, the cybersecurity of internet infrastructure and devices is crucial for physical security.

The ignorance of ordinary citizens while utilizing the Internet persists as a major concern. Cybersecurity, cyberlaw and digital literacy must be mandatorily incorporated at school and collegiate levels to increase the knowledge and awareness of end-users on internet usage and security. More awareness programs should be initiated by governments, civil societies and other stakeholders to increase society's awareness of concepts like cyber hygiene.

---

footnotes

7 https://en.wikipedia.org/wiki/Clearview_AI

8 https://money.cnn.com/2017/09/01/technology/china-alipay-kfc-facial-recognition/index.html

PROTECTION OF VULNERABLE GROUPS. The COVID-19 crisis has renewed and reinvigorated calls for the consolidation of human rights. We are thus of the position that policy makers must prioritize digital literacy as a tool to promote the rights of vulnerable groups on the Internet. Governments should invest in technologies such as broadcast white spaces alongside expanding fiberization to ensure accessible, inclusive and sustainable Internet access. To bridge the digital gap, they must also fund the provision of capacity-building efforts designed for marginalised communities.

However, access is no longer the only problem when addressing the issue of the Internet and human rights. Rather, the quality of access has also become a key issue. We believe that developing a human rights approach to internet governance is the best way to promote a free and open Internet that empowers vulnerable groups to flourish. Particularly in an environment where companies have few legal responsibilities, human rights infrastructure provides a way to organize and influence social pressure. Governments must create a clear set of standards well-informed by human rights due diligence for social media communication, and compel compliance. They should follow and evaluate the outcomes of social media regulation already executed in other countries and base domestic regulation on best practices. To complement this, social media platforms must articulate a policy that recognizes that systemic social inequality affects whose voices are heard and that speech on social media feeds and reinforces those underlying inequalities.