SURVEILLANCE TECHNOLOGIES AND HUMAN RIGHTS

Beyond the Security-Freedom Dilemma

Online Panel Event
14 June 2023

GENEVA CENTRE FOR HUMAN RIGHTS ADVANCEMENT AND GLOBAL DIALOGUE

GENEVA CENTRE FOR HUMAN RIGHTS ADVANCEMENT AND GLOBAL DIALOGUE

ONLINE PANEL EVENT

SURVEILLANCE TECHNOLOGIES AND HUMAN RIGHTS:

BEYOND THE SECURITY - FREEDOM DILEMMA

MODERATOR

Dr. Umesh Palwankar
Executive Director
Geneva Centre for Human Rights Advancement and Global Dialogue

SPEAKERS

Ms. Meredith Veit,
Tech & Human Rights Researcher,
Business and Human Rights Resource Centre;
USA

Mr. Sempala Allan Kigozi,
Tech Lawyer and a Digital Rights Activist,
Unwanted Witness;
Uganda

Ms. Tamar Kaldani,
Data Protection Consultant,
CoE, European Commission, GIZ;
Georgia

Dr. Catarina Fontes,
Postdoctoral researcher,
Institute for Ethics in Artificial Intelligence – Technical University of Munich;
Germany

Photo Credits: Canva - lukuntin77

Contents

FOREWORD

On 14 June 2023, the **Geneva Centre for Human Rights Advancement and Global Dialogue** held an online panel discussion on the human rights implications of surveillance technologies. Participants were invited to re-evaluate the usual "Freedom vs. Security" paradigm in light of the profound societal and cultural transformation that accompanied the widespread adoption of surveillance technologies in all sectors.

Approaching the new – and not so new – range of technological innovations for data-handling through the conceptual lens of 'surveillance' places our focus on the enhancement and redistribution of the power of information, and sheds light on the relationships generated between individuals, private organizations and States as subjects, suppliers, and consumers of information.

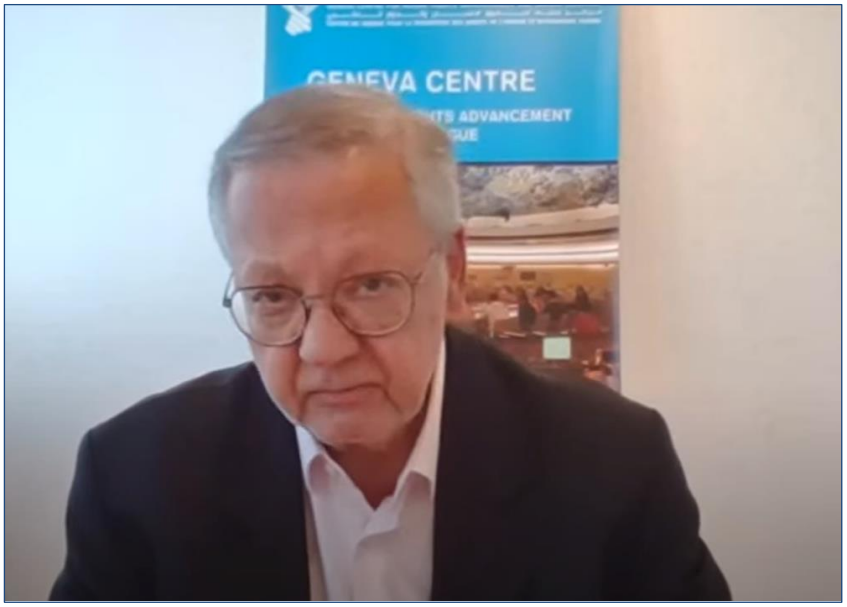
Ten years ago, Edward Snowden's revelations uncovered the secrecy in which intelligence agencies were conducting mass surveillance operations. Since then, surveillance technologies have become more sophisticated and, importantly, more accessible to a wider range of actors. Year after year, we've witnessed these technologies being used to target and silence journalists, dissidents, and human rights defenders. Products such as the Pegasus spyware abound in a growing obscure market. Consequently, this panel discussion constitutes an effort to inform readers of the ongoing debates and negotiations impacting human rights. It also aims to empower rights-holders in the face of concerning surveillance trends, and to call on duty-bearers to take positive action against any form of abuse. In the complex and rapidly evolving technology policy landscape, we urge decision-makers to remain committed to safeguarding human rights and fundamental freedoms.

In this spirit, the discussion benefited from the diversity of background and unique perspectives of our speakers. We sincerely thank them for sharing their insights and expertise with our audience and hope to build on the outcomes of this panel and progress towards a wider dialogue on the implications of digital technologies in all areas of human rights.

Dr Umesh Palwankar
Executive Director
Geneva Centre for Human Rights Advancement and Global Dialogue

PANEL STATEMENTS SUMMARY

Opening Remarks by Dr Umesh Palwankar, Executive Director of the Geneva Centre

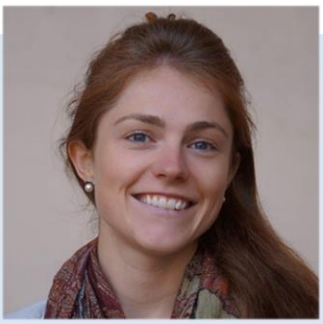


In his introductory remarks, Dr. Umesh Palwankar warmly welcomed the esteemed panelists, on behalf of the Geneva Center for Human Rights Advancement and Global Dialogue and his on his personal behalf. He thanked them for having accepted the invitation to this panel, in order to share their insights, their remarkable expertise, and https://gchragd.org/hands-on field experience at the international, national, and local levels.

He presented the agenda of the meeting consisting of identifying specific human rights risks, bring a better understanding of the obstacles and contentions regarding use and regulations, formulate clear recommendations in regard to international law based on the human rights perspective. Dr Palwankar also welcomed the attendants to the discussion, noting their enthusiasm participation from all regions of the world.

This meeting is the third panel the Geneva Centre has organized this year. The previous panels dealt with “Defending Women and Girls' Rights to Education, Challenges and Perspectives”. and “Interfaith Dialogue and Reconciliation, Creating and Sustaining Spaces of Encounter.” He warmly invited all participants to visit the Geneva Centre’s user-friendly website https://gchragd.org/

Meredith Veit, Tech & Human Rights Researcher at the Business and Human Rights Resource Centre



Ms. Veit's work sits at the intersection of business, human rights and technology, with a particular focus on at-risk groups. She is a journalist by vocation, and she has worked on various projects related to the protection of human rights defenders, journalists, migrants' rights and children's rights in the digital age. She specializes in fact-finding, trauma-informed and gender-sensitive interviewing, and project management. Ms. Veit holds a master's degree in human Rights and Democratization from the Global Campus of Human Rights and a bachelor's degree in Communication and Public Culture from George Washington University.

Ms. Veit presented the work of the Business and Human Rights Resource Center, which collects data on the human rights impacts of over 10,000 companies worldwide, engaging with companies and investors to urge them to share more information about how they're working to prevent and mitigate human rights harms and remediate where necessary.

The BHRRC made over 6,000 information requests across a number of sectors, and their website is a database where they collect allegations made against companies and their responses to those allegations. For the tech sector, the BHRRC website features tech company dashboards, which includes company's financial info, details of lawsuits over alleged human rights violations, available benchmark rankings, including digital rights rankings, the Corporate Human Rights benchmark[i],the Know the Chain[ii] benchmark, and others. The organization is also tracking allegations against industry actors that are involved in the overall surveillance architecture; companies selling invasive tech like spyware, including NSO Group, FinFisher, Gamma Group; companies providing a range of goods and services that include but are not limited to surveillance tech like Alphabet and Amazon; and companies that are producing goods and services that can be used for both surveillance and non-surveillance purposes. The BHRRC informs investors that have surveillance tech companies within their portfolios about the associated salient human rights risks.

Looking at surveillance tech's impacts on at-risk groups across a diversity of contexts, one example can be public housing facilities across the United States and local officials within those communities installing powerful and pervasive surveillance systems, according to a *Washington Post* investigative piece[iii]. These CCTV systems are funded through federal crime-fighting grants but are actually imposing an outsized level of scrutiny on some of the country's poorest citizens and disproportionately impacting minority groups. Some of these cameras are equipped with facial recognition and other artificial intelligence capabilities, but there's no guidance or limit on their use, and there's little evidence that they're actually making communities safer.

[i] Research and data for this benchmark are provided by the EIRIS Foundation, the Business & Human Rights Resource Centre, and two ESG intelligence provider: RepRisk and Vigeo Eiris.

[ii] KnowTheChain is a collaborative partnership between the Business & Human Rights Resource Centre, Humanity United, Sustainalytics, and Verité that provides resources for companies and investors to understand and address forced labor risks within their global supply chains.

[iii] MacMillan, D. (2023, May 16). Eyes on the poor: Cameras, facial recognition watch over public housing. Wasington Post. https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/

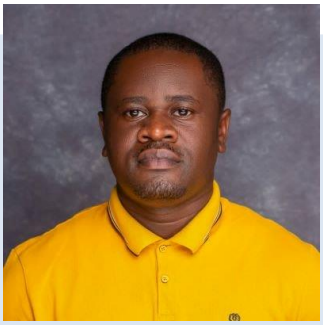
Instead, surveillance footage is being used to track minor infractions of residents to evict people. In North Dakota (U.S.A) officials have installed 107 cameras to watch 100 residents, which is a ratio of cameras per capita similar to the infamous Rikers Island jail complex in New York. This raises the question as to why this is happening and how these types of communities can hold companies to account.

Other examples of database inputs that demonstrate the flawed security - freedom dichotomy include cases in Iran where police are deploying surveillance tech to identify and prosecute women who breach the hijab law. In Palestine, tech companies are facilitating the implementation of the apartheid system according to Amnesty International reports. In Myanmar, tech companies are allegedly helping the junta build a surveillance infrastructure. In the United Kingdom, “dystopian” workplace surveillance system is disproportionately targeting young female and minority workers. In Egypt, digital rights groups are getting more and more concerned over fundamental freedoms as tech companies are building up the new administrative capital smart city. In Mexico, there are instances of spyware and targeting of human rights actors, including most recently from the report of Citizen Lab, the person who's coordinating the work of the country's Truth Commission investigating the Dirty War.

Ms. Veit added that people on the move, particularly asylum seekers and refugees, are highly vulnerable to rights abuses linked to the irresponsible deployment of surveillance technologies from companies such as Airbus, Nexa Technologies, Cellebrite, Irisguard, and Thales Group.

Finally, to further the conversation, Ms. Veit mentioned the Business and Human Rights Resource Centre and Unwanted Witness’s advocacy during the Summit for Democracy in March 2023, in favor of the US federal government's executive order on spyware.

Allan Sempala Kigozi, Tech Lawyer and a Digital Rights Activist at Unwanted Witness



Allan Sempala Kigozi has been at the heart of campaigns that promote the right to privacy and free expression both online and offline, and is a strong enthusiast of internet governance. He's an expert on the intersection of technology, law, and human rights. He is currently the head of legal programs at Unwanted Witness, where he has led advocacy campaigns, research interventions, capacity building workshops, and strategic litigation aimed at the realization of human rights and good governance.

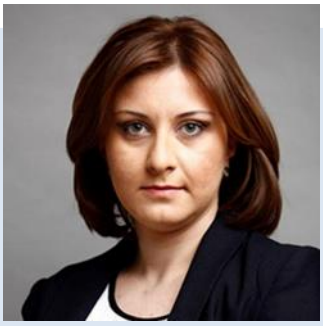
Mr. Kigozi introduced his organization, Unwanted Witness, which was founded to promote online freedoms and protecting digital rights in Uganda. Unwanted Witness aims to create a safe and secure digital environment for citizens and to promote responsible use of technology. Mr. Kigozi explained that surveillance, both online and offline, carries several risks for regular people. One of the most important being invasion of privacy. Surveillance allows certain parties to access private information, monitor people's activities, and the communication they have with others without consent. This intrusion into private life can have emotional and psychological consequences. Surveillance also poses the challenge of data breaches and identity theft. Surveillance systems may store a vast amount of personal data, making it a potential target for hackers. Once the systems and data are put in place, hacking into these systems becomes within reach for many. Telecom companies in Uganda share a lot of data with the National Identification Authority, responsible for registering and giving national IDs to citizens. The National Identification Authority has previously been the target of hacking. This occurrence is not unique to Uganda. In several countries many telecoms or even the national registers for national ID have been targeted. When these systems are compromised, individual sensitive information such as financial details, passwords, social security numbers can be stolen and can be misused for theft, especially identity theft and fraud.

Surveillance technology is also related to issues of free speech. The knowledge of being under surveillance can have a chilling effect on how people express themselves out of fear of potential repercussions. This has, in a way, stifled creativity, innovation and open discourse. Reputation damage also constitutes a major issue. Information collected has been used against government workers or political leaders. On accountability and effective redress in the case of privacy violations, strong privacy laws and regulations can help mitigate human rights risks. Mr. Kigozi recommended that governments adopt robust privacy laws that are clear and define individual rights and organizational obligations. In most countries, and in the case of Africa, current laws have glaring loopholes which data collectors have used to avoid accountability, without due regard for the privacy of the data subjects.

Mr. Kigozi also recommended independent data protection authorities to ensure accountability. These institutions should have the power to investigate, conduct audits, and impose penalties for noncompliance. Guidance should also be provided to organizations and individuals on privacy based practices. Mr. Kigozi highlighted the power imbalance between under-resourced Data Protection Authorities (DPAs) and data collecting entities enjoying high informal power and influence and extensive rights. He added that, in Africa, redress is difficult to obtain in part because DPAs are not independent, making it easy to circumvent their scrutiny. And in a way, many rights are infringed because of the weaknesses of DPAs. In addition, we need

transparent privacy policies. Privacy policies must be easily understandable in how they collect, use, and share personal data. They should also provide information on individual rights and procedures to file complaints or seek redress in case of any privacy violations. Informed consent and data minimization are also important principles to be applied. Most importantly, security measures should be implemented. For Mr. Kigozi, an essential requirement to be able to collect data is to possess adequate security capacities to protect it. He also identified a lack of proper notifications protocols in case of data breach. Lastly, public awareness is primordial. Unwanted Witness has run several campaigns to foster a privacy-conscious culture.

Tamar Kaldani, Data Protection Consultant



As a data protection consultant, Tamar Kaldani currently acts as data protection expert of the 'GLACY+' project of the EU and the Council of Europe, senior data protection expert for Africa of the European Commission project "International Digital Cooperation- Enhanced Data Protection and data flows", and team leader of the GIZ-commissioned project supporting the build-up of the Kenyan Office of the Data Protection Commissioner.

Tamar served as a First Vice-Chair of the Consultative Committee (T-PD) of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). As Georgia's first Data Protection Commissioner, she established the independent supervisory authority and developed it during two consecutive terms from 2013 to 2019. She holds LL.M and MBA degrees and is a Certified Information Privacy Professional/Europe (CIPP/E) from the International Association of Privacy Professionals (IAPP).

Ms. Kaldani shared that governments and private companies across the world are investing significant resources in developing and deploying surveillance technologies with AI being increasingly implemented in this market: According to Statista, the global surveillance technology market was valued at over 130 billion USD last year and the annual growth rate is 14-15 percent.[iv] Recent revelations and the examples that was shared even by previous speakers raise legitimate concerns about our privacy and other fundamental human rights. We as a civil society and citizens are also concerned with the reliability and security of those since even very progressive and useful innovations are accompanied by some risks, and if not regulated and managed properly, the mass surveillance technologies and predominant nature of AI systems with all these predictive and tracking abilities can significantly affect our fundamental human rights.

Concerns about national security and criminal activities may justify the use of surveillance technologies, and law enforcement services could have the legitimate aim to obtain the necessary information swiftly by using interception, facial recognition systems or AI's predictive ability to prevent crime or combat the threats related to national security. However, even states' wide-ranging discretion in the area of national security is not uniformly broad and states are bound by international, regional, and national human rights instruments. They have negative and positive obligations to safeguard individuals, including from actions by known state actors. Therefore, human rights should be at the center of any discussion or decision-making related to surveillance technologies. At the Council of Europe level, Article 8 of the European Convention on Human Rights and the relevant jurisprudence of the European Court provide clear guidance and interpretations regarding the possible restriction of the right to privacy. First, restrictions should be provided by precise, clear, accessible, and foreseeable laws. The development of surveillance methods or technologies, especially resulting in masse data collection, must be accompanied by a simultaneous development of legal safeguards securing respect to the essence of the fundamental rights and freedoms: It is necessary in a democratic society. States have to

[iv] Surveillance technology market size worldwide 2026. (n.d). Statista. Retrieved July 9, 2023, from https://www.statista.com/statistics/1251839/surveillance-technology-market-global/

demonstrate proactively the legitimacy, necessity, and proportionality of surveillance with regard to legitimate objectives that should be in direct connection with pressing public needs including public safety and crime prevention. European Convention, European Court judgments, resolutions of the Parliamentary Assembly including 2045 resolution on mass surveillance, and recommendations of the Committee of Ministers provide the legal instruments to ensure this. Moreover, Convention 108 - which is a landmark instrument since 1981 and the only legally binding international treaty in the data protection field, ratified by 55 parties, including nine European member states - set the basic principles for data protection safeguards for individuals, and for supervision over the data processing operations to deal with the challenges of a modern data-driven and digital world. Modernized Convention 108 reaffirmed the importance of these original principles and laid down the nuance, including transparency, accountability, privacy by design, and the need for human rights and privacy impact assessments that are particularly relevant in the context of surveillance technologies. The Convention also provides individuals with rights including in automated decision-making or profiling context. It is important to recall that contrary to previous provisions of Convention 108, parties to the modernized Convention will no longer be able to exclude from the scope of replication of the Convention certain types of processing such as for national security or defense. The possible exceptions to a limited number of principles such as transparency are subject to special conditions and in any case, independent and effective review and supervision should be guaranteed. The Modernized Convention also reinforced the investigative and corrective powers and independence of Data Protection Authorities and enhanced their international cooperation and opportunities for joint action. But the level of transparency and public scrutiny in the application of surveillance technologies are still limited. Independent and effective supervision plays a critical role in building trust and balancing interests at stake. The Council of Europe Convention 108 Committee also offers various practical guidelines that are particularly relevant in this context. For example, guidelines on AI, facial recognition or the practical guide on the use of data in the police sector. There are a set of guidelines that address developers, manufacturers and service providers. Those guidelines emphasize the role of different actors, including civil society, that have to ensure the protection of our rights and fundamental freedoms and prevent dangerous outcomes both at individual and societal level. Finally, people embrace data-driven innovations and technologies only if they're confident that their data is processed in a lawful, fair and proportionate manner. Therefore, effective safeguards and credible oversight systems should be in place to enable the identification of unlawful activities and ensure that those responsible are held accountable. Transparency and accountability create a foundation for trust and along with compliance with data protection legal frameworks. Codes of ethics, and certification mechanisms could also help to enhance this trust.

Echoing Mr. Kigozi's comment, she added that DPAs should have corrective enforcement and investigative powers and resources to exercise and supervise the implementation of data protection legal frameworks effectively. They should also have resources and capacities for awareness raising and to be part of all discussions related to technologies that affect the whole of society and should be consulted prior to deployment any mass surveillance technology. DPAs should look into the implementation gap that exists between the law on paper and reality on the ground. Remedies should be effective, proportionate and dissuasive. There are many promising developments, at the Council of Europe level as well as at the EU level, to come up with a solid legal framework on AI. Other initiatives exist such as the General Data Protection Regulation (GDPR) which has a very positive effect on the development of national data protection laws. According to Professor Graham Greenleaf, in 2023, there are 162 countries with data protection laws and 70 plus with data protection bills. Most of these laws and bills are modeled after the GDPR and Convention 108+. There are positive developments for global convergence.

Catarina Fontes, Postdoctoral Researcher at the Technical University of Munich

Dr. Fontes is a postdoctoral researcher at the Technical University of Munich. She works directly with Christoph Lütge, Professor and director of the TUM Institute for Ethics in Artificial Intelligence, and an interdisciplinary team of researchers on the research project Ethics for the Smart City. Applied socio-technical frameworks to assess the implementation of AI-related solutions. One of her research topics is the use of intrusive surveillance technologies in public spaces and impacts for individuals and society. Dr. Fontes holds a PhD in Urban Studies granted by the New University of Lisbon and University Institute of Lisbon.

Dr. Fontes presented some insights drawn from the research project Ethics for the Smart City.[5] Today, not only cam our footprints in the physical world be tracked, but also our digital footprint in the cyberspace. Traces of our online presence are under surveillance with or without our awareness. How artificial intelligence affects surveillance and privacy, leveraging data, namely personal data, became a very pressing matter for individuals and society. The aforementioned research project looks at the implementation of remote biometric identification systems by public authorities in public spaces and for law enforcement purposes. Although human rights are definitely a baseline to discuss surveillance and privacy issues, the discussion should move beyond human rights into the ethical development and implementation of surveillance systems to make sure that they align with democratic values and that we can protect our democracies from such systems.

The most well-known biometric identification system is the face recognition system that has already been tried within and outside Europe and followed by significant backlash from civil society organizations and also activists. In response, many cities banned the use of this technology and at the EU level there are significant efforts to regulate the implementation of remote biometric identification systems in publicly accessible spaces. Technology keeps pushing the boundaries of what society thinks is acceptable, but why are remote biometric identification systems in order to support the enforcement of the law considered inacceptable in public spaces? First, it challenges the principle of fairness. Namely, it will be overexposing certain vulnerable groups to surveillance such as children, people living in the streets, street vendors, street artists, among many other groups. And this may mean that refusing being under surveillance in public space will become equivalent to giving up access to these spaces. This contravenes the inclusivity of public space, potentially promoting the exclusion of groups particularly exposed or vulnerable to surveillance. Second, it challenges the principle of autonomy. We already assume that there is a certain level of transparency from the public authorities when implementing surveillance systems, yet the question remains on whether autonomy can be safeguarded without questioning consent as one of the core topics.

Consent actually goes beyond awareness. It implies an action of agreeing and simultaneously creating a path to withdraw it. Also, if the values at stake are presented as unquestionable, the possibility of a diverse opinion is conditioned and the autonomy to make an uncoerced choice is hindered. So, if a technology that relies on the intrusion of individual privacy is presented by public authorities as the most suitable solution to societal problems, such as criminality or terrorism, the request for consent is blurred by the apparent lack of arguments to decline it. Third, we should consider the principle of non-maleficence So there's the risk that mass and automated surveillance will be naturalized. This may radically affect the way societies function and potentially undermine democracies. Naturalizing the use of intrusive surveillance systems can create a

[v] see here: https://www.mos.ed.tum.de/en/vvs/forschung/projekte/ethics-for-the-smart-city/

chilling effect, leading to the loss leading us towards coerced societies with individuals having their rights and autonomy suppressed. So, to prevent the banalization of the adoption of intrusive surveillance systems and abusive use of personal data, there is the need to raise awareness of public authorities and populations about the benefits, but also the threats that these systems represent while empowering both to be able to discuss trade-offs.

QUESTIONS & ANSWERS

Question: ***Why is international cooperation in the field of cybercrime and data protection so crucial to protecting the rights of peoples? What are the main obstacles in getting national legislations to comply with international law?***

Tamar Kaldani: Indeed, cooperation is essential and when data flows have no geographic boundaries, national or regional solutions are important, but not sufficient. As a first state Data Protection Commissioner for Georgia, I have seen firsthand that with no leverage over multinational companies, there were cases where I had to use cooperation platforms and bilateral formats to ensure at least some remedies for the individuals affected. Honestly, we were not always successful in our endeavors due to the differences in legal systems or limited abilities to obtain the necessary information in a timely manner or conduct joint investigations with other regulators. Besides the very important policy work carried out by the European Data Protection Board, the Global Privacy Assembly and other regional networks of the data protection authorities like in Africa or the American network, we see now the clear focus on the practical and more pragmatic sides of cooperation, which is mutual assistance, joint investigations, and enforcement.

Another important point is that we really need convergence between different legal regimes. Privacy is a fundamental human right and no matter in which jurisdiction my data is processed, I desire the minimum safeguards. Data should be processed lawfully and proportionately. In addition, unfortunately, the revelations that we've all seen concerning the surveillance technologies show that people who have nothing to do with any type of criminal activities and wrongdoings are subject to constant monitoring, including of their behavior and communications.

We have seen many scandals related to unlawful data processing of politicians, human rights defenders, activists, and lawyers. And besides the direct effect that it has, we have to think about the chilling effect on millions of ordinary citizens who live in constant fear that their communications, images, locations, movement, interactions are under constant monitoring.

It's not only about privacy. It's about our dignity, and our other essential human rights, including freedom of expression. That's why I think that there is a need at the regional and international level to agree on commonly acceptable standards. I believe that Convention 108+ really creates this ground to be seen as a global standard. Let me also highlight that there are 55 parties to the Convention. Out of them, 9 are non-Council of Europe members and more countries could be invited considering this convention is setting the minimum basic standards that will be commonly acceptable everywhere.

With regard to cybercrime, more than 68 countries are parties to the Budapest Convention on Cybercrime and Privacy and its protocols, and 20 more either signed or are invited to accede to this international instrument. I believe this also creates this common ground for convergence as well as cooperation. Cooperation has very practical aspects when it comes to data protection authorities and it also has different dimensions when it comes to effective safeguards and addressing common challenges, including in the field of cybersecurity.

Question: ***What aspects should be considered when deciding upon the adoption or authorization of surveillance technologies, including those using AI-enabled systems?***

Catarina Fontes: Well, surveillance technologies can mean a lot of things and we have to see who is putting forward these kinds of initiatives. If it's public authorities, they have specific purposes. So, I think it's always very important to think about who is doing it and for what purposes it has been implemented. We also know that surveillance has other faces that are even more obscure than what we see nowadays with, for example, facial recognition in public spaces. And it is even more concerning because awareness and transparency are completely not there. There are many angles that we need to just identify and tackle when talking about surveillance technologies and we shouldn't' put everything at the same level or in the same bag because

risks are different and also benefits are diverse. We could also talk about the case of face recognition or other biometric identification systems for the purpose of crime prevention. In this case, I believe that they are presenting very high risks for democratic values and also for individual rights because it is overexposing all citizens to this kind of surveillance, independently of them being under suspicion or not. We are not just tracking criminals; we are monitoring all citizens for no justifiable purpose. This changes the way societies live because we do not usually live under this pressure of being monitored in public spaces. And if we are under this kind of premise, I think there will be a naturalization of surveillance that is quite dangerous for prevailing democratic values, and it is more so linked to authoritarian regimes.

Question: ***Could you elaborate further on the loopholes present in data protection laws and how they have been exploited?***

Allan Sempala Kigozi: The data protection system that we have largely in Africa was brought in from the GDPR *(EU General Data Protection Regulation)* and not so much from the African continent context. So, much of what privacy means in Europe is not what it means in Africa. For instance, in Uganda, there is no proper distinction and knowledge of what amounts to a data collector. So, anyone can easily be a data collector and the same level as a telecom company. For example, because of the phone I have which contains phone contacts, many of the laws in Africa would refer to me as a data collector. With laws that are not so comprehensive, it has been so very easy for manipulators and even governments to use it to surveil citizens.

For instance, governments have what they usually call national security. They can access data using new ways of collecting or processing data and sometimes they refer to national security. This vagueness and ambiguousness make it very easy for governments to, in any way, collect your personal data even without consent. They will collect it and process it in a way that isn't considered fair. There is no guidance on what national security means exactly which gives a lot of powers to enforcement. In most African countries, with reputation laws, governments can easily, go ahead and collect massive amounts of data.

In Uganda, we currently have the National Identification Authority, the agency in charge of collecting personal information for identification purposes. It's now sharing this massive data with telecom companies. As much as there might be a benefit with sharing this data with telecom companies, such as easier identification, the risks associated with that are huge. They do this without a privacy impact assessment or proper transparency. For instance, do these telecom companies have sufficient security measures to collect, to store and possess this information? Because there are already precedents where telecom companies in Uganda - and this is true to also other African countries - have been hacked into. Now, a telecom company accessing ID information, can complete engage in profiling of individuals, eroding their privacy entirely. People can be surveilled, monitored, their movements and activities can easily be monitored too because information from the telecom company, national ID, biometrics, location, all together amounts to complete profiling.

People who utilize personal data are so resourced that the punitive measures that are put in the law are not scaring them at all. In Europe, when you look at the GDPR, their sanctions are a bit high. So it makes people think twice before they want to infringe or use personal data without consent. In Africa, the laws are not as punitive.

DPAs (*Data Protection Authorities*) are not as independent as they should be. For instance, in Uganda, the DPA has only six staff members to supervise the entire country. That's unbelievable. Such loopholes in data protection laws have made it very easy for governments to perform massive surveillance and profiling of its citizens.

Question: ***What has been gained through the new U.S Intelligence Authorization Act and the new US executive order on spyware?***

Meredith Veit: The executive order on spyware from the Biden administration that was published in March of this year and has significant carve-outs and gaps in terms of enforcement, given its nature of executive order. It only applies to federal agencies and there are carve-outs for national security, but this is one of the most advanced and promising developments in relation to accountability of spyware technologies and surveillance tech companies. And one of the most promising pieces of this is that there was an active engagement across multiple agencies within the U.S government, which is not always a given, because the U.S government is not a monolith of actors. They were actively engaging with other allied governments in order to sign onto similar human rights due diligence practices and trying to identify which companies are affiliated with human rights harms, both domestically and abroad.

It is yet to be determined how well this is actually going to be implemented. It's not exactly clear as to how transparent the processes or results will be but in such an opaque space as the proliferation of spyware, this is a promising development.

The Business and Human Rights Resource Center was involved with a number of other actors in order to raise the concerns ahead of the Summit for Democracy with over 40 other digital rights groups from around the world, talking about how we need more coordinated action. The surveillance technologies really are incurring borderless problems when it comes to human rights harms, especially for vulnerable groups. And we need more scrutiny for investors. We need to be able to more clearly follow the flow of money for who is investing in these surveillance tech products and how they're being developed. We also need more of an emphasis on know-your-customer due diligence and scrutinizing the end use of specific technologies, which is something that is now currently under deliberation within the corporate sustainability and due diligence directive in the European Union. When it comes to corporate accountability for the tech sector, we are very happy to see that there is a stronger focus on stakeholder engagement between the impacted groups, especially groups in the Global South who are being victimized by some of the technologies and the tech companies that are being developed in the Global North.

There are also discussions about what investors' roles should be in this. Unfortunately, due to some lobbying efforts, there have been more questions than there should be about whether or not investors are companies or firms that have influence within this space.

Question: ***How does the Business and Human Rights Resource Centre mechanism work and how do you source information?***

Meredith Veit: I invite everyone to have a look at the database because you can see our timelines where we log everything into Stories. We source information through our partners that are distributed around the world. We specifically look at local and regional CSOs, journalists and think tanks that are involved in conducting a lot of this research. We also publish reports from academia. We use these third party reports as a way to reach out to companies when they are not responding to those groups, acting as a kind of intermediary, we're more able to pull their responses into one place, publish them in full so that the companies are having their voices heard, in comparison to the allegations. These are public documents that CSOs can use also as a way to build for their campaigns and advocacy work. And it can be used as evidence if there are any cases that are brought forth and related to these allegations. I will leave it for the audience to have a look and see the quality of the responses from some of these companies. It varies across the board. Sometimes we get one or two sentence replies. Sometimes we get three-page explanations with links.

Question: ***Are there any specific recommendations regarding the use of multimedia tools that enable biometric recognition and hence subsequently potentially put at risk some stakeholders engaging with some organizations?***

Catarina Fontes: Actually, biometric identification is quite a simple process. Usually, governments have some watch lists of suspects that should be tracked. And then the images that are recorded in real time in public spaces are scanned with the help of an A.I and it identifies - it does the matches - with the dataset or this watch list. The same can be done with video recordings.
I would recommend keeping this data safe and storing it in a way that can be protected from being hacked or being accessed by other third parties.

LESSONS LEARNED AND WAYS FORWARD

Beyond the Security – Freedom Dilemma

Surveillance, in the context of this discussion, refers to close observation and monitoring of people, behaviors, objects and spaces. It implies the extraction, storage, processing, and sharing of data.
Leveraging "tech for good" has been a central consideration and a major selling point for the mainstreaming of surveillance technologies, but documented and repeated human rights abuses raise questions on the risks these technologies generate for fundamental rights and freedoms. While it doesn't necessarily constitute a breach of privacy, the expansive deployment of surveillance technologies and their embeddedness into most aspects of private and public life engender information asymmetries and shifts in power. Debates around surveillance reached a new momentum during the COVID-19 pandemic when new digital platforms were established by governments in order to combat the spread of the virus. The adoption of contact tracing apps and digital vaccination verification systems were a critical aspect of the public facing COVID response across many countries, sometimes leading to abuses by authorities.
The idea underpinning the expansion of surveillance is that more – and better – data ensures safety and security[6]; or more broadly, enables better risk management [7]. This extends beyond national security into many areas of life, such as healthcare, financial services, or business.

At present, surveillance no longer serves the sole purpose of strengthening security. Big data - larger data sets of a greater variety and velocity - offers new opportunities for information gathering and research, thereby informing policymaking. Former United States Secretary of the Treasury Lawrence Summers described data collection as the "ultimate public good" [8], driving scientific progress and uncovering unknown relationships. Through this angle, divulging personal information and adding to a larger collection of data can be construed as an act for the benefit of society at large.
At the same time, this framework implies that individuals should forgo parts of their privacy and stake other rights and freedoms that intersect with it for the sake of security and development.[9] Overarching rights include, the right to freedom of opinion and expression, the right to freedom of peaceful assembly and association, and the right to access to information. Against this concern, the 'nothing to hide, nothing to fear' argument obviously stands weak considering the far-reaching societal implications of surveillance and the many contexts in which it manifests. Without the possibility to fully consent in an informed manner and with insufficient transparency on surveillance practices, it is not necessary to have 'something to hide' to fear one's information may be used to stifle the free exercise of their rights or the rights of others, especially journalists, parliamentarians, justices, or human rights defenders.

However, there has been significant efforts to formulate this debate beyond the perceived dilemma. The first UN Special Rapporteur on the right to privacy Prof. Joseph Cannataci wrote in his first report to the Human Rights Council: "[…] it is not helpful to talk of 'privacy versus security' but rather of 'privacy and security', since both privacy and security are needed. Both rights can be taken to be enabling rights rather than ends in themselves. Security is an enabling right for the overarching right to life, while privacy may also be viewed as

[6] Cavoukian, A. (2017) "Global privacy and security, by design: Turning the "privacy vs. security" paradigm on its head". Health Technol. 7, 329–333. https://doi.org/10.1007/s12553-017-0207-1
[7] Lyon, D. (2003). Surveillance Technology and Surveillance Society. In T. J. Misa, P. Brey, & A. Feenberg (Eds.), Modernity and Technology (pp. 160–184). MIT Press.
[8] Summers, L. H. (2016, April 4). Data collection is the ultimate public good. Financial Times. https://www.ft.com/content/6d3d019e-9a31-33b7-a7ec-e79f4f108aa0
[9] Lyon, D. (2017). Digital citizenship and surveillance| Surveillance culture: engagement, exposure, and ethics in digital modernity. International Journal of Communication, 11, 19.

an enabling right in the overall complex web of information flows in society, which are of fundamental importance as regards autonomy and the ability of individuals to identify and choose between options in an informed manner as they develop their own personality throughout life."[10]

In the current context of an ever-evolving technological landscape, surveillance capabilities have outpaced the laws regulating them[11]. Also bearing in mind the cross-border nature of digital data, the debate becomes geared towards questions of data ownership, purpose limitation of surveillance technologies, and responsibility sharing. Who owns information? Who determines what should be done with it? How do we ensure it is used within reasonable boundaries, and with due regard to human rights?

Surveillance technologies, deployment, and use

Surveillance is a broad term that encompasses a variety of systems that employ technologies together or separately to collect data about individuals, places, trends, and relationships. They do not pose an evident risk In and of themselves without considering their primary or secondary purpose, their deployment and applications.

Among the technologies and systems posing significant challenges for privacy and other human rights:

- Biometric technologies refer to facial or voice recognition, fingerprint or iris scanning, and other technologies that can identify individuals based on innate characteristics. Biometrics are used in national identification systems or in the workplace to monitor attendance for example.

- **Video surveillance**, which can be in closed-circuit (CCTV) or cloud-based, and is also more and more often enhanced by AI.

- **Location monitoring technologies**

- **Deep Packet inspection** technologies are used to monitor internet traffic by viewing the content of packets (blocs of data) and where it came from. They can also redirect network traffic. Their primary purpose is to detect and block viruses and other undesirable packets.

- **IMSI catchers** simulate cell towers and intercept phone traffic. They collect information on the device that is connected to the catcher unbeknownst to its user.

- **Data Analytics** technologies discover patterns and can piece together data to provide information about behaviors or relationships between data subjects.

- **Intrusion technologies** are able to access and/or control a device remotely without the user's knowledge.

- **Artificial Intelligence** can instantly generate insights on large amounts of data, boosting surveillance and analysis performance of many other technologies.

Surveillance technologies aren't only deployed on mobile or computer devices. Devices like wearables (for example fitness watches) or home security systems extract and store personal data as well. The advent of Big Data, AI and the Internet of Things further enabled a multipurpose and interconnected collection and interoperability of data. Surveillance technologies also realize enhanced capabilities to sort and analyze data

[10] UN Human Rights Council, 'Report of the Special Rapporteur on the Rights to Privacy', 31st Session of the Human Rights Council (2016), A/HRC/31/64, para. 23

[11] Decuyper, A. (2016). On the research for big data uses for public good purposes: Opportunities and challenges. Netcom, 30-3/4, 305–314. https://doi.org/10.4000/netcom.2556

so that even information that is made public and thrown in an ocean of similar data can be processed and interpreted to fulfill a variety of purposes.

When using digital platforms or through offline activities that involve digital platforms, users explicitly or tacitly accept a number of conditions and give 'permissions' which authorize access, sharing, and storing of a range of personal data. On digital devices this can include viewing network connections, accessing contact lists, browsing history, and fine locations among other things. On mobile applications, some permissions are built-into the software development kits (SDKs) developers use to create applications. They automatically transfer data to the third party providing the SDKs, namely event data such as when the app is installed and when it is used.[12] Applications and websites also contain third-party trackers, meaning certain data collected is instantly shared with those third parties. While a certain amount of disclosure is required in this regard, the lack of transparency regarding who data is shared with and how it is processed by third parties has been decried by many privacy advocates. In addition, the terms and conditions allowing such access can usually be accepted in a single click, giving the option to skip over what would otherwise be a long and vague description of privacy policies. Unwanted Witness conducted an analysis on an Bible reading application, showing 15 trackers that collect personal data and process it according to their own privacy policies.[13] In 2018, an analysis of 959,426 Google Play apps found that they included on average 10 trackers; and 18% of them included more than 20 trackers, associated to 5 companies on average.[14] Several anonymization or pseudonymization techniques are employed to protect privacy, however it remains possible to re-identify data subjects by piecing together disaggregated data.[15] Encryption methods are key to avoid identification and secure data[16], although all methods present limitations and have vulnerabilities.

Surveillance is most commonly noticed by the general public in the context of targeted advertising. Digital information gathered about an individual - one's digital footprint - can be pieced together to create profiles and identify them. This is done in part when data collected by one party is shared with other parties using advertising IDs (such as the Google's AAID and Apple's IDFA) which enable advertisers to link data about user behavior from different apps and web browsing into a comprehensive profile.[17] Businesses can use the data they directly gathered from their customers or third party data, obtained from different sources, to gain insight on behaviors and preferences and tailor their marketing accordingly[18]. This means users will be offered ads depending on their gender, age, or ethnicity but also spending habits, residence location, and relationships[3]. As a result, ads presented are more relevant to the user and certain groups can be excluded from certain content (children with alcohol ads for example).[19] In addition, companies such as Google and Microsoft use

[12] How apps on android share data with Facebook. (2018). Privacyinternational.org. https://privacyinternational.org/sites/default/files/201812/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf

[13] Unwanted Witness. (2021, November 25). Pocket spy: How your smartphone helps companies track your digital footprint. https://www.unwantedwitness.org/pocket-spy/

[14] Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018). Third party tracking in the mobile ecosystem. In SocArXiv. https://doi.org/10.31235/osf.io/u7qmz

[15] Decuyper, A. (2016). On the research for big data uses for public good purposes: Opportunities and challenges. Netcom, 30-3/4, 305–314. https://doi.org/10.4000/netcom.2556

[16] Encryption brief. (2018, June 11). Internet Society. https://www.internetsociety.org/resources/doc/2018/encryption-brief/

[17] Ibid

[18] Data and Marketing Association, 2018, Dma Advice: Using Third Party Data Under The GDPR, https://dma.org.uk/uploads/misc/third-party-data-guide-1.0.pdf

[19] Fourberg, N., Serpil, T. A. Ş., Wiewiorra, L., Godlovitch, I., de Streel, A., Jacquemin, H., Hill, J., Nunu, M., Bourguigon, C., Jacques, F., Ledger, M., & Lognoul, M. (2021). The impact of targeted advertising on advertisers, market access and consumer choice. Europa.Eu. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662913/IPOL_STU(2021)662913_EN.pdf

real-time bidding systems where ads are bought and sold each time an online site is loaded[20], transmitting users' information on what they view online and their real-time location to other advertisers and to publishers. According to the Irish Council for Civil Liberties, this constitutes a massive data breach where people's information is exposed several hundred times a day to thousands of companies and potentially intercepted by unknown data collectors.[21] These interceptors can be data brokers, companies that buy and analyze data to profile users, and sell this information again, across borders and to a variety of buyers. Through this segmentation of data, advertisers are able to target vulnerable groups or persons based their emotional states, their financial difficulties etc.… Questions can be raised on how expansive access to personal data enables advertisers to conduct manipulative or predatory marketing tactics. A case study on for-profit colleges and universities in the United States suggests that these institutions use digital advertising based on data analytics to target single-parent household living close to the poverty line.[22] This same study referred to leaked Facebook documents, revealing in 2017 that the company "offered a top Australian bank the opportunity to advertise to Australian kids, college students, and young workers at vulnerable emotional moments—when they felt 'insecure,' 'need[ed] a confidence boost,' or felt 'anxious'.[23] These insights have the potential to maximize revenue for businesses, making data more valuable than ever. According to Statista, the global big data market size was estimated at 70 billion USD in 2022 and is forecasted to grow to 103 billion USD by 2027.[24]

The same data that is collected en masse on digital platforms informs more than advertising. Lending or insurance decisions are increasingly based on varied personal data elements collected from various sources and sometimes processed and supplied by data brokers. A large variety of data elements such as spending habits, number of times a persons moved, smartphone usage etc.… factor into determining the creditworthiness of individuals.[25] This practice involves partnerships between start-ups using data analytics technologies, banks or financial service providers such as MasterCard, credit reporting companies and sometimes mobile network providers. These new ways of judging creditworthiness have the potential to perpetuate discriminatory biases against the most vulnerable groups[26] by capturing disadvantaging characteristics stemming from structural inequalities. The same practices are present in the insurance sector where unregulated algorithms use data to determine insurance rates.[27]

Personal data also plays a key role in the health sector. The amount of data collected about individuals and most importantly the innovative ways in which it is processed have shown potential to improve health services. Electronic Health Records (EHRs) are the most common tools in this regard, storing individual's medical history and sharing it across different health service facilities to improve healthcare delivery in a

[20] Kerry, C. F., & Robison, M. (2022, December 5). Rulemaking in privacy legislation can help dial in ad regulation. Brookings. https://www.brookings.edu/articles/rulemaking-in-privacy-legislation-can-help-dial-in-ad-regulation/
[21] Lomas, N. (2022, May 16). Report spotlights vast scale of adtech's 'biggest data breach.' TechCrunch. https://techcrunch.com/2022/05/16/iccl-rtb-report-google-gdpr/
[22] Gilman, S. (2019). Proliferating predation: Reverse redlining, the digital proliferation of inferior social welfare products, and how to stop it. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3511892
[23] Levin ,S. Facebook Told Advertisers It Can Identify Teens Feeling 'Insecure and Worthless', GUARDIAN (May 1, 2017), https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens
[24] Global big data industry market size 2011-2027. (n.d.). Statista. Retrieved July 17, 2023, from https://www.statista.com/statistics/254266/global-big-data-market-forecast/
[25] Christl, W., & Spiekermann, S. (2016). Networks of control: A report on corporate surveillance, digital tracking, big data & privacy (1st ed.). Facultas.
[26] Melendez, S. Now wanted by big credit bureaus like Equifax: Your 'alternative' data, FastCompany (June 4, 2019), https://www.fastcompany.com/90318224/now-wanted-by-equifax-and-other-credit-bureaus-your-alternative-data
[27] Probasco, J. (23 June 2022) "The insurance industry confronts its own racism", Investopedia. https://www.investopedia.com/race-and-insurance-5075141

personalized manner. These individual records are aggregated and analyzed by private companies to inform decisions on treatment or even predict health risks and patients' behaviors towards drugs.[28] A McKinsey report mentions, for example, the company Asthmapolis which uses "GPS-enabled tracker that records inhaler usage by asthmatics. The information is ported to a central database and used to identify individual, group, and population-based trends. The data are then merged with Centers for Disease Control and Prevention information about known asthma catalysts (such as high pollen counts in the Northeast or volcanic fog in Hawaii). Together, the information helps physicians develop personalized treatment plans and spot prevention opportunities"[29]. Other big-data applications include the use of wearables that enable users to track various aspects of their health.

This raises salient privacy concerns are this vulnerable information will not only be susceptible to hacking but also illustrate a trend of for-profit public-private partnerships in the health sector.[30]
The COVID-19 pandemic also prompted the launch of several contact tracing apps by governments[31] that use location data with the aim of limiting disease transmission. Introduced in conjunction with emergency laws around the globe, these apps raised concerns about privacy and security. In the United Kingdom, "the development of a contact tracing app by the National Health Service was met with concerns from parliamentarians about the lack of legal protections and clarity in terms of what data would be collected, what that data will be used for, who will have access to it, and how it will be safeguarded from hacking". [32]

On the government side, government agencies directly gather and store personal information through a variety of channels, including public services and public administrations. We observe more and more public-private data sharing as governments attempt to harness the full potential of data for decision-making.[33] Business-to-government data sharing and other public-private partnerships are particularly relevant regarding the mushrooming smart city projects that not only require an great amount and variety of data, but are also designed to generate new – and very profitable – data on its residents[34], thus, raising questions on the extent and purpose of public-private partnerships .

Governments also largely make use of biometrics, namely for National Identity Systems. This provides individuals with a digital identity to access public and administrative services among other things. The complete effectiveness, inclusiveness, and security of these identity systems are paramount to the full realization of their civic rights.

On March 2023, France became the first EU country to adopt a law legalizing AI-enabled facial recognition. [35]Biometrics and other forms of surveillance technologies coupled with access to a growing amount of data

[28] Kayyali, B., Knott, D., & Van Kuiken, S. (2013, April 1). The big-data revolution in US health care: Accelerating value and innovation. Mckinsey.com; McKinsey & Company. https://www.mckinsey.com/industries/healthcare/our-insights/the-big-data-revolution-in-us-health-care
[29] Ibid
[30] Digital Health: what does it mean for your rights and freedoms. Privacy International, from https://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rights-and-freedoms
[31] Sun, N., Esom, K., Dhaliwal, M., & Amon, J. J. (2020). Human rights and digital health technologies. Health and Human Rights, 22(2), 21–32.
[32] Ibid
[33] Guidance on private sector data sharing. (n.d.). Shaping Europe's Digital Future, from https://digital-strategy.ec.europa.eu/en/policies/private-sector-data-sharing
[34] Mercille, J. (2021). Inclusive smart cities: Beyond voluntary corporate data sharing. Sustainability, 13(15), 8135. https://doi.org/10.3390/su13158135
[35] 'All-out assault on privacy': France is first EU country to legalise AI-driven surveillance. (2023, March 29). The Brussels Times.

and metadata are increasingly used by law enforcement and intelligence agencies, with the aim of national security, counter-terrorism, and cybercrime fighting; a trend largely documented in the latest report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.[36]

Authorities not only access data held by the governments, but occasionally turn to commercial surveillance tools that monitor public databases such as social media. Data collected through smartphone applications can, for example, be accessed and analyzed by law-enforcement or for criminal investigation,[37] which surpasses the simple interception of communications. [38] To this end, data retention policies allows or requires telecommunication companies to store information of their customers for a defined amount of time.[39] A range of technologies and methods such as facial recognition, wiretapping[40], or web scraping create a situation of indiscriminate mass surveillance where data is collected and filed without prior investigation. To maximize the availability of data and analytic capabilities, law enforcement agencies occasionally work with private companies. For example, in 2020 it was found that a company named Clearview AI provided access to law enforcement agencies to a facial recognition platform, using a database of over 3 billion images extracted from open websites.[41] The company was faced with three lawsuits in three U.S states.

Recently, Amazon has come under fire for directly marketing a facial recognition product called Rekognition to law enforcement agencies for use in conjunction with police body cameras, which would allow police to identify people in real time. The product was piloted with police departments in Orlando, Florida and Washington County, Oregon.

AI surveillance technology is spreading at a faster rate to a wider range of countries than experts have commonly understood. At least seventy-five out of 176 countries globally are actively using AI technologies for surveillance purposes.[42]
Social media platforms are considered to be “thermometers” measuring people’s sentiments and gathering information for behavior predictions.[43]

Human Rights Risks

Surveillance technologies pose salient human rights risks and are too often used to undermine fundamental

https://www.brusselstimes.com/430820/all-out-assault-on-privacy-france-is-first-eu-country-to-legalise-ai-driven-surveillance

[36] United Nations, Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/52/39 (1 March 2023)

37 Ringrose, K., & Ramjee, D. (2020-2021). Watch Where You Walk: Law Enforcement Surveillance and Protester Privacy. California Law Review Online, 11, 349-366.

38 United Nations, Human Rights Council, Report of the Special Rapporteur on the right to privacy, A/HRC/34/60 (6 September 2017), available on undocs.org/en/ A/HRC/34/60.

39 Ogasawara, M. (2022). Legalizing Illegal Mass Surveillance: A Transnational Perspective on Canada’s Legislative Response to the Expansion of Security Intelligence. Canadian Journal of Law and Society / La Revue Canadienne Droit Et Société, 37(2), 317-338. doi :10.1017/cls.2022.9

[40] Ibid

[41] Miyamoto, I. (2020). Surveillance technology challenges political culture of democratic states. Hindsight, Insight, Foresight, 49-66.

[42] Feldstein, S. (09.2019). The Global Expansion of AI Surveillance. Carnegie Endowement for International Peace.

[43] Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society, 12(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

rights and perpetrate cycles of violation and abuse.

The general public commonly faces privacy risks associated with hacking and unauthorized access to data. In the United States, 5,150 healthcare data breaches of 500 or more records have been reported to the Office for Civil Rights between 2009 and 2022 exposing 382,262,109 healthcare records.[44] In 2023, *the Independent* reported a cybersecurity attack affecting the data of 1 million patients in the United Kingdom, many of which unaware of the risks as they did not need to give consent to be recorded on the dataset. While security challenges are inherent to surveillance technologies, private and public entities must ensure their compliance with data protection policies to limit risks of attacks. Many countries have institutions conducting regular audits and investigations in this regard.[45]

Coupled with advanced analysis technologies, mass surveillance methods can be strategically used on particular groups to augment capacities for identification and profiling. This translates into higher and undue levels of surveillance of certain groups, hence perpetuating discriminations. Furthermore, the introduction of A.I in many facial recognition systems adds a layer of risk. Several studies have shown that A.I is inherently biased because it is based on historical data, resulting in discrimination based on ethnicity, gender, age and other identity factors. Although there are constant advances in A.I technologies, solving biases in algorithms is likely mathematically impossible.[46] Many studies focused on the United States testify to the inaccurate profiling leading to the false arrests of individuals from ethnic minorities, often of African or Asian descent.[47] As discussed by Meredith Veit during the panel discussion, facial recognition and other forms of mass surveillance are disproportionately deployed in low-income areas. Low-income households are also subjected to higher monitoring (biometrics data, drug tests etc..) in order to access welfare programmes. This information feeds into police systems, leading to a cycle of surveillance.[48] Once again the multipurpose collection of data winds up having greater consequences for vulnerable groups.

Surveillance technologies enable predictive and as such more preemptive policing, leading to a logic of deterrence and incapacitation rather than proportionate punishment.[49] [50] Hence, mass surveillance methods, such as bulk interception of communication, facial recognition or bulk collection of metadata, can have a chilling impact on free expression, association and access to information. A survey of 1212 respondents testing the chilling theory found that the awareness of being surveilled promoted caution and self-censorship, even more so when there was a knowledge that targeted action could be taken in response to online activity.[51]

---

[44] Healthcare data breach statistics. (2023, May 21). HIPAA Journal. https://www.hipaajournal.com/healthcare-data-breach-statistics/

[45] OECD. (2020). Oversight bodies for access to information. In Review of the Kazakhstan Commission on Access to Information. OECD.

[46] Townson, S. (January 26, 2023). Manage AI bias instead of trying to eliminate it. MIT Sloan Management Review. Retrieved July 24, 2023, from https://sloanreview.mit.edu/article/manage-ai-bias-instead-of-trying-to-eliminate-it/

[47] Chin, C., & Lee, N. T. (2022, April 7). Police surveillance and facial recognition: Why data privacy is imperative for communities of color. Brookings. https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/

[48] Privacy and welfare surveillance among vulnerable communities - information saves lives. (2020, January 16). Information Saves Lives | Internews. https://internews.org/commentary/privacy-and-welfare-surveillance-among-vulnerable-communities/

[49] Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Big Data & Society, 1(2), 205395171454186. https://doi.org/10.1177/2053951714541861

[50] Van Brakel, R., & De Hert, P. (2011). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. In E. de Pauw, P. Ponsaers, K. Van Der Vijver, W. Bruggeman, & P. Deelman (Eds.), Technology-led policing: Journal of police studies (pp. 163–192). Maklu, Uitgever.

[51] Penney, J. W. (2017). Internet surveillance, regulation, and chilling effects online: a comparative case study. Internet Policy Review, 6(2). https://doi.org/10.14763/2017.2.692

Importantly, the broad and vague language that is often used in legislation particularly concerning national security, counterterrorism and cybersecurity[52] can give extensive prerogatives to law enforcement agencies to use advanced and invasive technologies abusively.[53]

Invasive technologies have been routinely used against protesters without a clear investigation purpose.[54] These practices are widespread not only in the context of major political unrest, but for all sorts of large of mega-events such as the Winter Olympics in Canada and the G20 summit in the United Kingdom where many protesters were arrested and fined on the basis of unsubstantiated suspicions[55] rather than for committing actual offences. In 2023, France doubled down on this trend and became the first E.U country to adopt a plan to install A.I enabled cameras for the duration of the 2024 Olympic Games and until the end of 2024 at least. [56]

Unbridled government access to privately-held and commercial data is a growing feature of state surveillance programs around the world. Mandatory or voluntary data-sharing from private companies has been implemented in many countries, expanding the availability of personal data for law enforcement and intelligence purposes. In the United States, Privacy International[57] reported that several contracts were made between the company Amazon and local law enforcement to give them access to video recording from Amazon's safety doorbell 'Ring', without needed consent from users in exchange for the police departments promoting the product to communities.

In addition to data-sharing, states impose data retention periods to telecom companies. Although this practice has been found unconstitutional in many countries, France is a European exception, being the only country where police can access data stored by telecom companies – for at least a year – without any judicial authorization.[58] The UAE presents another case of opaque data sharing and retention regulation. It has only two licensed telecom companies, both majority state-owned and which are required to filter the content of data flows "in line with the priorities of the state." Data-sharing is agreed upon through private discussions between the Telecoms and Digital Government Regulatory Authority and the companies.[59]

Journalists, human rights defenders, political dissidents and even justices or parliamentarians are especially vulnerable in the face of mass and targeted surveillance technologies. In targeting the most vocal and outspoken categories of people; people who are responsible for sharing information and represent the

[52] See Joint Statement UN Twentieth Anniversary Joint Declaration: Challenges To Freedom Of Expression In The Next Decade and UN Joint Declaration on Freedom of Expression and countering violent extremism;
https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/JointDeclaration10July2019_English.pdf
https://www.ohchr.org/en/statements/2016/05/joint-declaration-freedom-expression-and-countering-violent-extremism?LangID=E&NewsID=19915

[53] See Statement of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism at the 49th session of the Human Rights Council, 15 March 2022
https://www.ohchr.org/sites/default/files/2022-03/2022-03-10-Statement.pdf

[54] n [40]

[55] n [50]

[56] 'All-out assault on privacy': France is first EU country to legalise AI-driven surveillance. (2023, March 29). The Brussels Times.
https://www.brusselstimes.com/430820/all-out-assault-on-privacy-france-is-first-eu-country-to-legalise-ai-driven-surveillance

[57] One Ring to watch them all. (n.d.). Privacy International. Retrieved July 26, 2023, from https://privacyinternational.org/long-read/3971/one-ring-watch-them-all

[58] Ali, Z. (2022, January 21). Mandatory data Retention Around The World. BeEncrypted.
https://beencrypted.com/privacy/laws/mandatory-data-retention/

[59] Rizvi, R. (2021, June 24). In brief: telecoms regulation in United Arab Emirates. Lexology; Simmons & Simmons.
https://www.lexology.com/library/detail.aspx?g=037b66f1-f1f8-4e75-9539-d08528a94397

interest of a larger group, the civic space will be adversely impacted, hence the rights of entire societies are threated. In infamous case of the Pegasus spyware, sold by the Israeli company NSO group, has uncovered the ability of governments, and potentially other actors, to spy on individuals without having them perform any action on their devices.[60] The proliferation of these types of technologies is even more alarming considering the record number of journalists jailed in 2022, amounting to 533 according to Reporters Sans Frontières.[61] Governments are also using these tools to targeted civil society. In 2018, the Indian government jailed 16 human rights defenders, on account of 'unlawful activities'. The prosecution presented evidence that was found to be planted through malicious software onto dome of the defenders' computers.[62]

Migrants also count among the most targeted groups by extreme surveillance practices. In the United States, the Immigration and Customs Enforcement agency imposes location tracking technologies on migrants and asylums seekers as part of the Alternatives to Detention programme. Migrants assigned to the programme must either wear a GPS ankle monitor with 24/7 location tracking, use a phone reporting system with voice recognition, or a smartphone app that uses facial recognition software and GPS location. The app is operated a subsidiary company of the GEO Group, a private prison company.[63] These methods are clear infringements of migrants' dignity and privacy, and it is unclear how the data collected could be used or shared in the future. In the European Union, the borders have become more and more militarized. The European Border and Coast Guard Agency (Frontex) has the mandate to buy and rent its own equipment, with an 845.4 million EUR budget for the year 2023,[64] concluding profitable contracts with companies in the military industry such as Airbus and Elbit Systems.[65] The agency uses drones provided by these companies to monitor the Mediterranean. A Human Rights Watch report strongly indicates these drones have been used to stop boats carrying migrants and refugees and help Libyan authorities intercept them, capturing more than 32,400 migrants in 2021.[66] In addition, the European border control infrastructure makes heavy use of biometrics. Frontex has been collecting the fingerprints of migrants and storing them in the EURODAC the asylum fingerprint database.[67] Access to this database is being extended to non-EU States such as Albania, Serbia and Bosnia-Herzegovina were privacy and data regulations are not harmonized with EU standards. The European Commission's

[60] Pegasus Project: Apple iPhones compromised by NSO spyware. (2021, July 19). Amnesty International. https://www.amnesty.org/en/latest/news/2021/07/pegasus-project-apple-iphones-compromised-by-nso-spyware/

[61] New record number of journalists jailed worldwide. (14 December 2022.). Rsf.org. https://rsf.org/en/new-record-number-journalists-jailed-worldwide

[62] Action needed to address targeted surveillance of human rights defenders. (2021, December 2). Front Line Defenders. https://www.frontlinedefenders.org/en/statement-report/action-needed-address-targeted-surveillance-human-rights-defenders

[63] Hellerstein, E. (1 May 2023). Immigrating to the US? ICE wants your biometrics. Coda Story. https://www.codastory.com/authoritarian-tech/us-ice-alternatives-to-detention/

[64] European Border and Coast Guard Agency. (n.d.). European Union. Retrieved August 7, 2023, from https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/frontex_en

[65] Frontex's contracted companies reportedly operating surveillance equipment to monitor migrants & refugees crossing the Mediterranean; (1 March 2022). Business & Human Rights Resource Centre. https://www.business-humanrights.org/en/latest-news/frontexs-contracted-companies-reportedly-operating-surveillance-equipment-to-monitor-migrants--refugees-crossing-the-mediterranean-utilized-by-the-israeli-military-in-its-assaults-on-gaza-incl-co-responses/

[66] Airborne Complicity. (2022, December 8). Human Rights Watch. https://www.hrw.org/video-photos/interactive/2022/12/08/airborne-complicity-frontex-aerial-surveillance-enables-abuse

[67] Submission to European Commission consultation on "security-related information sharing" (29 March 2023). Statewatch.org. https://www.statewatch.org/analyses/2023/submission-to-european-commission-consultation-on-security-related-information-sharing/

proposal for reciprocal access for frontline officers in the EU and key partner countries to be adopted end of 2023, would further extend this practice to other countries provided "minimum conditions and expectations from the EU side concerning data protection and fundamental rights standards" are met.[68] This poses obvious concern given Frontex's abuse record part and the lack of human rights standards implementation in many countries who would potentially meet those standards on paper. Data-sharing collection and data-sharing by border control agencies – without the consent of migrants and asylum seekers – can be used to prosecute them and hinder their right to seek asylum. After complaints have been made about Frontex's debriefing interview practices to the European Ombudsperson, they found that the agency had no recorded proof of consent to record interviews and retain them. The complainants warned that the information gathered was shared with Europol as well.[69] Amidst the appalling loss of many migrants at sea, Frontex continues to strengthen its surveillance capabilities through information-sharing arrangements with countries across Europe and Africa private contract with influential military companies. Thus, A.I systems are more and more sought after.

The EU A.I Act represents a crucial development in this area. Currently in the trialogue negotiation phase, the bill is not only decisive for migrants, who are often targeted by profiling through surveillance, but everyone. Currently the text as amended states that "This Regulation shall not apply to public authorities in a third country nor to international organisations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations use AI systems in the framework of international cooperation or agreements for law enforcement and judicial cooperation with the Union or with one or more Member States […]".[70]

Mass surveillance frequently intertwines in areas experiencing systemic and acute oppression and repression. For instance, the Committee on the Elimination of Racial Discrimination raised concerns over China's collection of biometric data and phone scanning in the Xinjiang Uygur Autonomous Region[71] where the government runs a campaign of mass incarceration and internment. Perhaps one of the most jarring cases of leveraging surveillance against a population is that of Israel. The UN Special Rapporteur on Human Rights described the Occupied Palestinian Territories as an open-air *panopticon*[72] in her latest report to the Human Rights Council. The use of drones, facial recognition, systemic tapping of phones and monitoring of phone and internet communication Israel is designed to nip in the bud any attempt to legitimately resist foreign occupation and generates a feeling of omnipresence meant to dissuade any contestation.[73] The face recognition system 'Red Wolf' and related 'Blue Wolf' app and 'Wolf Pack' database are some of the tools operated by the Israeli military to forcibly photograph Palestinians, including children,[74] and capture their biometrics at checkpoints

[68] European Commission - Have Your Say. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13243-Security-related-information-sharing-%E2%88%92-reciprocal-access-for-frontline-officers-in-the-EU-and-key-partner-countries_en

[69] European ombudsman. (3 July 2023.). Europa.Eu. https://www.ombudsman.europa.eu/et/decision/en/171951

[70] Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))

[71] UN Committee on the Elimination of Racial Discrimination, 'Concluding observations on the combined fourteenth to seventeenth periodic reports of China (including Hong Kong, China and Macao, China)', (2018), CERD/C/CHN/CO/14-17

[72] UN Human Right Council, Report of the Special Rapporteur on the situation of human rights in the Palestinian territory occupied since 1967 (2018), A/HRC/53/59

[73] Shtaya, M. (n.d.). Nowhere to hide: The impact of Israel's digital surveillance regime on the Palestinians. Middle East Institute. Retrieved July 26, 2023, from https://www.mei.edu/publications/nowhere-hide-impact-israels-digital-surveillance-regime-palestinians

[74] Abukhater, J. (2022, April 13). Under Israeli surveillance: Living in dystopia, in Palestine. Al Jazeera. https://www.aljazeera.com/opinions/2022/4/13/under-israeli-surveillance-living-in-dystopia-in-palestine

of even from their own homes.[75]

In China, the treatment of the ethnic Uyghur minority is appalling as well. Special procedure mandate holders and the Committee on the Elimination of Racial Discrimination have raised concerns about the use of such technologies in the Xinjiang Uyghur Autonomous Region in the context of the application by China of its Counter-Terrorism Law and its implementing measures in the region.[76]

Key Principles and Human Rights Safeguards

International law

The fundamental right to privacy is enshrined in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, as well as a number of regional legal instruments including the European Convention on Human Rights and the American Convention on Human Rights, and regional non-binding instruments.

At present, most countries have included the right to privacy in their constitution or domestic law (137 according to UNCTAD[77]), but legal provisions and case law on data privacy, corporate surveillance, national security, and cybersecurity remain widely disparate. However, the trans-border nature of dataflows implies that protection of privacy rights and other overarching rights necessarily require the harmonization of legal frameworks. So far, no international legally binding instrument on data privacy or surveillance exists. In 2018, the former UN Special Rapporteur on the Right to Privacy proposed a "Draft Legal instrument on Government-led Surveillance and Privacy"[78] which was the product of multistakeholder consultations and several research projects. However, the text did not find much support in the Human Rights Council and some States expressed the view that there were no gaps in international law in this area.[79] Similarly, a global civil society coalition launched "International Principles on the Application of Human Rights to Communications Surveillance" were finalized in 2013 following consultations with experts, including the UN Special Rapporteur on the Right to Freedom of Expression and Opinion.

The Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (CoE Convention 108+) is the only legal text that can claim a universal vocation.[80] The original Convention is ratified by 55 States including 10 non-members of the CoE while the modernized version – the protocol amending the Convention – has 27 ratifications including from 9 non-members. The Convention was modernized to align more closely to the European Union's Geneal Data Protection Regulation (GDPR) but has a more comprehensive scope, applicable to all data processing activities including in the fields of justice,

[75] Israel/OPT: Israeli authorities are using facial recognition technology to entrench apartheid. (2023, May 2). Amnesty International. https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/

[76] See communications CHN 18/2019 and CHN 14/2020; and CERD/C/CHN/CO/14-17, para. 40 (b).

[77] Data Protection and Privacy Legislation Worldwide. UNCTAD. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[78] see Draft Legal Instrument: https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf

[79] Talmon, S. (5 June 2018,). No need for legal instrument on electronic surveillance and privacy. GPIL - German Practice in International Law. https://gpil.jura.uni-bonn.de/2018/06/no-need-legal-instrument-electronic-surveillance-privacy/

[80] de Terwangne, C. (2021). Council of Europe convention 108+: A modernised international treaty for the protection of personal data. Computer Law and Security Report, 40(105497), 105497. https://doi.org/10.1016/j.clsr.2020.105497

combating crime, defense, public safety and State security.[81]

For its part, the GDPR is considered as the golden standard in the field of data protection. It replaced the EU Data Protection directive and strengthened many of its provisions notably by imposing more stringent obligations[82] on controllers (those who decide how and why the data will be processed) and processors (those who process the data on behalf of the controllers). The General Regulation also makes remarkable strides in terms of transparency by imposing information be provided to the data subjects regarding the contact details of the data protection officer; the period of storage or criteria used to determine that period; whether communications or transfers are planned and the regulations authorizing such communications or transfers; the right to lodge a complaint with a supervisory authority; whether communication is a statutory or contractual requirement, or is necessary to enter into a contract, and whether the subject is required to provide his or her personal data and the consequences of a failure to do so; the existence of automated decision-making, including profiling, meaningful information about the logic involved, and the significance and envisaged consequences of such processing; and information on the purpose when further processing is planned for a purpose other than that for which the data were collected.[83] Albeit ambitious, the guarantees contained in the GDPR present significant challenges in national adaptation. Dr. Karen McCullagh, Dr. Olivia Tambou and Sam Bourton' s book on illustrates the issues faced regarding the readability of the European model as formulated in the General Regulation.

It is important to note that the legal frameworks presented here only cover personal data and does not apply to legal entities such as corporations, institutions and non-governmental organizations. The GDPR defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"[84] If data has been transformed to no longer relate to a natural person, Recital 26 of the GDPR states : "Personal data which have undergone pseudonymization, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly." In cases where datasets contain a mix of personal and non-personal data that are inseparable, the Regulation on a framework for the free flow of non-personal data in the EU provides that the GDPR applies.[85] However, the distinction between personal and non-personal data can still be blurred in many instances. The adverse use of non-personal data relating to demographics of users or public spaces is left largely unaddressed in data protection frameworks.

The adoption of the GDPR in 2016 ushered numerous data protection laws around the world with the view of

[81] Ibid

[82] General Data Protection Regulation. Privacyinternational.org. https://privacyinternational.org/learn/general-data-protection-regulation

[83] UN General Assembly, 'Report of the Special Rapporteur on the Rights to Privacy', (2022), A/77/196, para. 54

[84] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1. Art. 4(1)

[85] Personal data and non-personal data: the differences. (2022, September 5). Lexology; Studio Legale Stefanelli & Stefanelli. https://www.lexology.com/library/detail.aspx?g=db2e2c36-deab-4c3a-b7e9-8aee31f70faa

obtaining a positive adequacy decision from the European Commission in conformity with to the Article 45 of the GDPR reading :"A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection".[86]

In Africa, the African Union's Convention on Cyber Security and Personal Data Protection (Malabo Convention) reportedly entered into force in June 2023,[87] gathering the 15 necessary ratification instruments 9 years after its adoption and becoming the first binding treaty on data protection outside of Europe. According to the NGO Data Protection Africa, 20 countries in Africa do not have data protection laws,[88] therefore the Malabo Convention is a promising opportunity to boost privacy rights across the continent.
The African Union also released its Data Policy Framework with the same goal of harmonization and with a view to support the setup of the digital economy in the continent while safeguarding human rights. It recognizes the need to adapt privacy laws to the African context and advances various models of data stewardship (for example data trusts).[89] It also approaches privacy not only as an individual right but as a community and collective rights issue.[90]

As another example of non-binding regional instruments, the Standards for Personal Data Protection of the Ibero-American Data Protection Network[91] provides a flexible model to design data protection legislation while identifying principles on data processing and outlining measures for proactive responsibility of data controllers and processors.

Regulatory frameworks are underpinned by common basic principles relevant to the regulation of surveillance. In her 2022 report to the General Assembly, the UN Special Rapporteur on the right to privacy identified 8 principles and analyzed their meanings[92] in various regulatory documents: legality and legitimacy, consent, transparency, purpose, fairness, proportionality, minimization, quality, responsibility and security.

The term 'legitimate interest' as a legal ground for the processing of data suggests a balancing between the interests of the data subjects and those of the controllers and third parties (whom data is shared with). The term encompasses a large spectrum of interests such as marketing[93], advertising, research or fraud prevention[94] as long as they do not violate the law.[95] In the GDPR, the interest of a data subject can override

[86] Geneal Data Protection Regulation. Art. 45
[87] Ayalew, Y. E. (15 June 2023). The African Union's Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond? EJIL: Talk! https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/
[88] Data Protection Africa. (2022, August 29). Data Protection Africa | ALT Advisory; ALT Advisory. https://dataprotection.africa/
[89] African Union (2022) Data Policy Framework, p.28. https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf
[90] Ibid
[91] Approved in 2017 by the the Ibero-American Network for the Protection of Data, an association of 22 Data Protection Authorities (DPAs) from countries in Central and South America, the Caribbean and Spain and Portugal.
[92] General Assembly, Special Rapporteur on the right to privacy (2022), A/77/196
[93] Recital 47, GDPR
[94] Ibid
[95] Kamara, I., & De Hert, P. (2018b. Understanding The Balancing Act Behind The Legitimate Interest Of The Controller Ground: A

that of the controller if "personal data are processed in circumstances where data subjects do not reasonably expect further processing."[96] On the contrary, it can be determined that a controller's interests overrides those of the data subjects. Such cases should be determined on an individual basis.[97] Naturally, national security constitutes a legitimate interest, which has often been used around Europe and the world to justify invasive mass surveillance. Even in the case of national security, other key principles should be upheld.

In connection to this principle of purpose and minimization where data can only be collected for a defined, legal and legitimate purpose, the principle of proportionality (or relevance) must be taken into consideration. The common practice of mass surveillance has been ruled inconsistent with this principle the European Court of Human Rights on many occasions if appropriate safeguards are not in place.[98] On the issue of accountability, it is important to keep in mind the innate information asymmetry between controllers and data subjects since the former design or chose and their own surveillance policies and understand better than data subjects.[99] For this reason, robust mechanisms should be established. According to the principle of security, measures should be taken to ensure the confidentiality, integrity and availability of personal data. This principle applies to organizations who have the duty to promptly patch vulnerabilities to cyberattacks.[100]

To ensure the full protection of rights under legal frameworks, sharing or transferring data to a territory under privacy and data protection laws judged inadequate can be facilitated by transfer tools containing appropriate safeguards. Under the GDPR, they include Standard data protection clauses (SCCs); Binding corporate rules (BCRs); Codes of conduct; Certification mechanisms; Ad hoc contractual clauses.[101] The Ibero-American Network for the Protection of Personal Data supports similar tools.[102]
https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf

In regard to monitoring mechanisms, the GDPR the Malabo Convention and CoE Convention 108+ require State Parties to setup independent national data protection authorities (supervisory authorities) to and lay out their powers and duties which include enforcement powers and the tasks to lodge complaints.[103] The UN General Assembly, in its resolution 69/166 called upon States to "establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of

Pragmatic Approach. Brussels Privacy Hub, Vrije University Brussels, 4(12), p.12

[96] Recital 47, GDPR

[97] European Commission. When can personal data be processed? (n.d.). https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en

[98] E.g Big Brother Watch and Others v. the United Kingdom. (2018) ECHR; Szabó and Vissy v. Hungary (2016) ECHR

[99] Andrew, J., Baker, M. (2021). The General Data Protection Regulation in the Age of Surveillance Capitalism. J Bus Ethics 168, 565–578 https://doi.org/10.1007/s10551-019-04239-z

[100] Maurushat, A., Nguyen, K. (2022) The legal obligation to provide timely security patching and automatic updates. Int. Cybersecur. Law Rev. 3, 437–465

[101] International data transfers. (n.d.). Europa.Eu. from https://edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en

[102] Cervio, G., Roth, M., Requejado, S., & Munoa, J. M. (2022, October 23). Multijurisdiction: Ibero-American Network for the Protection of Personal Data - Standard contractual clauses for the international transfer of personal data. Global Compliance News. https://www.globalcompliancenews.com/2022/10/23/multijurisdiction-ibero-american-network-for-the-protection-of-personal-data-standard-contractual-clauses-for-the-internal_10232022/

[103] Chapter VI (Articles 51 to 59) of the GDPR; Articles 11-12 of the Malabo Convention; Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (ETS No. 181)

communications, their interception and the collection of personal data". Independent and well-funded Data Protection Authorities (DPAs) play a critical role in ensuring compliance and access to effective remedies.

Legal frameworks on data protection largely do not apply to law enforcement and intelligence agencies. Many countries have oversight mechanisms for state surveillance regimes with varying procedures regarding officials' appointments and mandates. However, the conduct of law enforcement agencies and intelligence service remains loosely regulated, full of loopholes and lacking in transparency. The staggering technological advancements of surveillance technology innovations in the private sector are an enticing opportunity for governments to expand their surveillance arsenal. Thus, intelligence agencies request or require companies to retain and share the data they have extracted. [104] Through access to foreign privately-held data, governments are able to bypass their own domestic laws and gather information on their own citizen if their data was transferred across borders,[105] which is naturally often the case. As remarked by the OHCHR, "such practice arguably fails the test of lawfulness because, as some contributions for the present report pointed out, it makes the operation of the surveillance regime unforeseeable for those affected by it."
To address these growing trends, the Organization for Economic Co-operation and Development (OECD) became the platform for long negotiations resulting in the Declaration on Government Access to Personal Data Held by Private Sector Entities. The document adopts some basic data protection principles: legality, legitimate aim, data minimization, security, transparency, and effective redress, but allows flexibility. It only applies to direct access to privately-held data and not to surveillance activities a State might undertake abroad among intelligence agencies or on their own.

Often taking a security-first position, many States are currently pushing back against encryption, the conversion of plain information into secret code to ensure anonymization and secure data. As a Priva-enhancing technology, encryption is regarded as a crucial tool to guarantee the protection of fundamental rights. It is especially vital to journalists, human rights defenders, activists and other persons who exchange sensitive communications that are objects of repression and censorship. By extension, encryption is a technological tool to promote a free and democratic society where the right to information and the right to expression are fully realized.
While many countries do not have specific laws restricting encryption, law enforcement agencies may still require controllers to decrypt data, or they may have the prerogative to hack into systems.[106] Others have licensing policies for privacy-enhancing technologies that reject more advanced or performant forms of encryption. The NGO Access now argues on the other hand that encryption provides protection against the very threats law enforcement is combatting. [107]

Outside of the data protection and privacy framework, export control regimes in the field of surveillance stand as important tools to protect the rights of individuals outside a State's territory. Dual-use goods and

[104] Propp, K. (10 January 2023). Gentlemen's rules for reading each other's mail: The new OECD principles on government access to personal data held by private sector entities. Default. Retrieved August 3, 2023, from https://www.lawfaremedia.org/article/gentlemens-rules-reading-each-others-mail-new-oecd-principles-government-access-personal-data-held
[105] Ibid
[106] Chen, C. (29 September 2020). Losing the right to encryption means losing business. Internet Society. https://www.internetsociety.org/blog/2020/09/losing-the-right-to-encryption-means-losing-business/
[107] Björksten, G. (21 October 2021). Who we hurt when we attack encryption. Access Now. https://www.accessnow.org/who-we-hurt-when-we-attack-encryption/

technologies can be used for both civilian and military purposes and can be subjected to these regimes. These technologies with dual attributes can be used in war but also potentially against civilians. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Technologies is the only multilateral agreement that prevents the exportation of surveillance technologies. The agreement provides a list of technologies to 42 members who subsequently adopt domestic export control regimes over these technologies. The States members are urged to consider the risks if these technologies could be used 'to commit or facilitate the violation and suppression of human rights and fundamental freedoms'.[108]
Similarly, the European Union Dual-Use Regulation is a system which empowers Member States to control the export and transit of items not listed in the regulation if "the items in question are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law".[109]

Business and Human Rights

Understanding the global surveillance architecture and the interactions between its actors sheds telling light on the challenges to human rights. In our digital societies, the value of information continuously increases and the means to obtain it are increasingly sought after. As mentioned by Tamar Kaldani during the discussion, the market size for surveillance technologies was estimated at 130 billion USD in 2022.
Private companies, especially transnational corporations, have a key role in safeguarding fundamental rights and freedoms for their clients and the communities and individuals impacted by their activities. The current state of the surveillance industry, populated by diverse actors interacting in a complex regulatory landscape, entails a large degree of self-regulation.
Companies have responsibilities under international law and are expected to conduct due-diligence processes when developing and selling their products and services. The Guiding Principles on Business and Human Rights stated that "[I]n order to meet their responsibility to respect human rights, business enterprises should have in place policies and processes appropriate to their size and circumstances, including:
(a) A policy commitment to meet their responsibility to respect human rights.
(b) A human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights.
(c) Processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute". [110]
The Guiding Principles encourage businesses to engage in consultation with relevant stakeholders including civil society and human rights defenders and to communicate with national human rights information about how their address their human rights impacts. With no surprise, surveillance companies disclose little to no information about their activities.[111] On the other hand, thanks to relentless advocacy from civil society

[108] Wassenaar Arrangement, (2011) Explanatory Note 'Elements for Objective Analysis and Advice Concerning Potentially Destabilising Accumulations of Conventional Weapons'
[109] Regulation (EU) 2021/821 setting up an EU regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items Article 5.
[110] OHCHR (2011) Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. New York; Geneva
[111] The Global Surveillance Industry. (n.d.). Privacy International.

organizations, more tech companies engaging in surveillance such as Google (Alphabet) and Twitter have been consistent in releasing transparency reports.[112] Transparency report are intended to inform data subjects on the companies privacy policies and what actions are taken to uphold their responsibilities in regards to human rights.

For big tech corporations such as Amazon, Facebook or Google, transparency is all the more crucial given the amount of data under their control and their dominance in their markets. These corporations use third-party data from other businesses who use their SDKs and conduct activities through their platforms to gain unfair advantages and benefit their own businesses.[113] For instance in 2017, Google was fined 2.42 billion EUR by the by the European Commission for break anti-trust rules. Google was found to have included a number of criteria in these algorithms, to direct search traffic to its own comparison shopping service while demoting competitors. as a result of which rival comparison shopping services are demoted.[114] Given that the appetite for more and better data is intrinsic to their business models, controlling such large portions of data confers big tech corporations enormous influence of data subjects' environments and behaviors; what they see, learn, and consume.

Surveillance actors in the field of security and intelligence certainly grapple with less public attention, aside from a few infamous scandals. In this market, governments and intelligence agencies, intelligence and surveillance companies, tech companies, and hackers interact away from the public eye and sometimes on the black market, beyond the scrutiny of any authority. Surveillance actors also trade in computer- software vulnerabilities, a concerningly growing market.

Zero-day exploits, i.e., vulnerabilities in cybersecurity systems, are discovered by hackers or private intelligence companies like Fin Fisher and NSO Group, and sold to governments, intelligence agencies or other private entities. When an entity buys zero-day exploits, it has no way of knowing who else it has been sold to and whether or not there are the sole holder of the zero-day. This leads to an attitude of hoarding with the hopes of being a step ahead of competitors. Thus, the entire structure of the market is based on sustaining vulnerabilities and consequently undermining the security of the general public.[115]

Democratic and Rights-Based Approach to Surveillance

To what extent is the adoption of surveillance technologies the expression of a collective will? Could participatory decision-making shape the data governance models of tomorrow?

Overall, government and corporate surveillance practices lack transparency and effective human rights safeguards. Surveillance dynamics build in power imbalances and put data subjects in a position of individual

https://privacyinternational.org/explainer/1632/global-surveillance-industry

[112] Transparency reporting index. (2022, October 4). Access Now. https://www.accessnow.org/campaign/transparency-reporting-index/

[113] On the hypocrisy of using privacy to justify unfair competition. (n.d.). Privacy International. https://privacyinternational.org/news-analysis/4369/hypocrisy-using-privacy-justify-unfair-competition

[114] European Commission (27 June 2017) Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service. https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784

[115] Chaos Computer Club (26 November 2022), How to dry up the market for IT security vulnerabilities. https://www.ccc.de/en/updates/2022/zero-day-schwarzmarkt-trockenlegen

and collective vulnerability. American author Shoshana Zuboff incorporated the uneven relationship between data controllers and data subjects into the concept of 'data capitalism'.[116] The systematic accumulation of personal data about human experiences and its processing into behavioral data to predict and anticipate behaviors creates a relation of control. She equates it to a form of dispossession where people do not have access to the knowledge produced from the surveillance of their everyday lives. Conversely, innovative approaches are being developed to build participative and democratic data governance models in which benefits and control are shared.

The traditional reasoning tends to distinguish between governmental and private interests as two forces shaping and governing the implementation of surveillance,[117] assuming that one will act for public safety and security while the other will be driven by profit and the capture of market shares. Likewise, partnerships and data sharing agreements are typically only envisaged between private companies and governments. However, their interests often converge in opposition to citizens' interests.[118]

While there have been fruitful voluntary data sharing partnerships between private data-collecting companies and academic or public institutions, the final distribution of benefits is often ambiguous. It appears the sharing of privately-held data often involves pushing partners to generate additional data to be subsequently retrieved by the private company which ultimately deepens power imbalance. For example:

> *"Mastercard conducts data sharing initiatives under its Center for Inclusive Growth. In one important project, it has shared data with a trusted partner (the Urban Institute in Washington, DC, USA) to study urban displacement caused by development projects that could lead to gentrification. Mastercard used its residential cardholder zip codes to study cardholders' movements, for which available data were lacking."*[119]

Several proposals have emerged to establish data sharing models that empower people, especially the most vulnerable, to claim their rights and autonomy.
One of them is bottom-up[120]data trusts: legal entities in which a party or a group (beneficiaries) authorizes another, the trustee, to make decisions over their data on their behalf with the duty to protect their collective rights and best interests. Beneficiaries discuss and choose their data privacy preferences and the overall terms of the trust. In turn, the trustee is responsible for claiming the beneficiaries' rights and taking legal action on their behalf. Under these loose conditions, data trusts can be structured in different ways. Data is placed in a trust by a settlor. *A priori* the settlor would be the data controller, i.e., a company that collects data.
The advantage is that data trusts can be tailored for any data set and to serve any purpose, so an individual could join multiple trusts at different times, with the necessary condition of full data portability.[121] This

[116] Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. Journal of information technology, 30(1), 75-89.
[117] Mann, M., Mitchell, P., Foth, M., & Anastasiu, I. (2020). #BlockSidewalkto Barcelona: Technological sovereignty and the social license to operate smart cities. Journal of the Association for Information Science and Technology, 71(9), 1103–1115. https://doi.org/10.1002/asi.24387
[118] Mercille, J. (2021). Inclusive smart cities: Beyond voluntary corporate data sharing. Sustainability, 13(15), 8135. https://doi.org/10.3390/su13158135
[119] Ibid
[120] Delacroix, S., & Lawrence, N. D. (2019). Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance. International Data Privacy Law. https://doi.org/10.1093/idpl/ipz014
[121] Ibid

freedom should in theory confer a lot more autonomy and agency to individuals who would be able to pull their data into a legal entity with a stated economic or social goal (" data should be used to induce positive social change" or "advance health research") and re-establish balance between communities and companies. However, it appears many advocates of the data trust model envision it as a way to aggregate more data with a stamp of approval shielding companies from public criticism or political hurdles.[122] In fact, we can question what would incentivize data controllers have to set up these trusts in the first place if privacy law could, in principle, allow activities that the trust would potentially deny and impose prohibitions that are hierarchically superior to the consent of a trustee.[123]
The case of Sidewalk Lab smart city initiative in Toronto illustrates this concern. Sidewalk Lab, a subsidiary of Alphabet, planned to conduct a smart city development project on 5 hectares of land in the Quayside district in Toronto.[124] The project entailed mass data collection and surveillance so Sidewalk Lab launched the Urban Data Trust based on an open data model in which it claimed data would be de-identified by default and made publicly accessible with a view of sharing benefits. This raised many questions about privacy, oversight, and who would have effective control over the data.[125]The project was never completed and was met with a lot of outrage, leading to the #BlockSideWalk movement.

The stance behind this backlash is the rejection of private control over public spaces and the demotion of individuals as passive users.[126]. Furthermore, the terms in which public-private surveillance partnerships operate often involve massive technological input from the private side and reduced control over that input of democratic institutions. Against this backdrop, the concept of 'data sovereignty' or 'technological sovereignty' finds growing support as a framework for participative and democratic forms of data governance.[127] It refers in broad terms to the "ownership and control over personal data, and how technologies can be used to promote autonomy whether at an individual or collective level"[128]
There are still discussions as to how data sovereignty would be embodied in concrete settings. Barcelona's technological sovereignty initiatives since are a much-examined example in this regard. It was one of two European cities (with Amsterdam) to host the E.U project DECODE[129] which provided platforms for users to control their data and for communities to easily create services that respect users' rights. Users' private information is stored in personal 'wallets' and they are able to access services without this information being stored elsewhere.[130]

With concern for the economic viability of alternative data governance models, most trials so far relied on open-source digital development. There is still a lot of room for innovation and certainly challenges that have yet to be effectively addressed. A lot of emphasis has been placed on creating safer and fairer environments for sharing data among different actors, with little work done on more fundamental decisions

[122] O'hara, K. (2020). Data Trusts. European Data Protection Law Review. Volume 6, Issue 4 p. 484 - 491 https://edpl.lexxion.eu/data/article/16559/pdf/edpl_2020_04-005.pdf
[123] Ibid
[124] Vincent, D. (26 September 2019). Sidewalk Labs' urban data trust is 'problematic,' says Ontario privacy commissioner. Toronto Star, https://www.thestar.com/news/gta/sidewalk-labs-urban-data-trust-is-problematic-says-ontario-privacy-commissioner/article_ae44fec0-2180-58f3-8799-196a034707ce.html
[125] Ibid
[126] n (103)
[127] n (104)
[128] n (104)
[129] N (104)
[130] An introduction to DECODE. (2018, May 25). Nesta. https://www.youtube.com/watch?v=_-ooCbgIiyo

regarding the deployment of surveillance technologies. Ultimately protecting privacy and other human rights through local community-centered initiatives, private orderings, and other technical tools like end-to-end encryption can only yield positive impact if it is accompanied by important law reforms[131] that in places human rights at the center and addresses the unique implications of surveillance technologies.

Recommendations and ways forward

- **Strengthen oversight mechanisms.** This entails well-funded fully independent DPAs with corrective enforcement powers, stringent transparency and information provisions in law, and accessible complaint procedures. This is crucial not only for the sake of accountability, but because case law and precedents are a central way to delineate the principle of 'legitimate aim'.

- Require transparent and open **risk assessment processes** at all levels, and before deployment.

- **Promote legal and policy innovation.** This encompasses content-based innovation across national and international regulations, as well as community-led initiatives and proposals.

- **Respect the universality of the right to privacy**. States in particular should recognize the same rights of their citizens to all persons regardless of citizenship status, migrant status, or any other factors. For companies, it means applying the highest standards of privacy and security in all places of activity.

- **Uphold special protections for journalists** and others who share information.

- **Impose prompt software-vulnerability patching in digital systems**. Human rights in the digital age rely on the security of their personal data, so data controllers and processors should ensure it is safe at all times. The withholding of zero-day exploits by intelligence authorities puts the public at risk.

- **Make use of and execute export control regimes** to prevent human right abuses.

GENEVA CENTRE
FOR HUMAN RIGHTS
ADVANCEMENT AND
GLOBAL DIALOGUE

Rue de Vermont 37-39, 1211 Geneva 20, Switzerland
Tel:+41(0) 22 748 2780, info@gchragd.org