31/03/2023

Security Spirits

Issue 01

CONTENTS

WHO ARE WE?

IMSISS

The International Master in Security Intelligence and Strategic Studies is an Erasmus Mundus Joint Master's Degree (EMJMD) between the University of Glasgow (Scotland), Dublin City University (Ireland), Università delgi Studi di Trento (Italy) and Charles University (Czechia).

Students on this master's degree programme examine a broad range of contemporary security challenges and explore the intelligence and strategic approaches used by governmental and non-governmental actors to combat these threats.This degree adopts a unique approach to the study of security by combining theoretical, applied and empirical knowledge and skill sets.

For more information, click here.

THE SECURITY DISTILLERY

The Security Distillery is a student-run think tank founded by students of the 2017-2019 cohort of the International Masters in Security, Intelligence and Strategic Studies (IMSISS) programme, which is collectively awarded by the University of Glasgow, Dublin City University, University of Trento and Charles University Prague.

In the dynamic field of security studies, we intend to distil the essence of complicated issues into digestible amounts of comprehensible information, without oversimplifying or losing nuance. Our content is structured regionally and thematically.

"We aim to turn complex security issues into simple, quality, accessible information for students and researchers."

For more information, click here.

OUR PARTNERS

THE PRIVACY SALON

Privacy Salon is a Belgian NGO that aims at sensibilising and critically informing the broader public, policymakers, and industry about privacy, data protection, and other social and ethical issues that are raised with the introduction of new technologies in society. Privacy Salon is the organiser of the annual Computers, Privacy and Data Protection (CPDP) Conference in Brussels. The 16th edition of CPDP will be held from 24 to 26 May 2023, with a vibrant programme of more than 90 panel and workshop sessions on topics including privacy, data protection, new technologies and fundamental rights. Privacy Salon is the curator of the Data Art Guide (DAG) and the organiser of the Privacytopia festival, with its first edition taking place in Ghent in March 2024.

For more information, click here.

CPDP CONFERENCE

The Computer Privacy and Data Protection conference (CPDP) has been organised since 2007. It is the most important conference in Brussels for the professional and research community in the field of computers, privacy and data protection, hosting more than 400 speakers and 85 panels over 3 days each year. As a world-leading multidisciplinary conference, CPDP offers the cutting edge in legal, regulatory, academic, and technological development in privacy and data protection. CPDP gathers academics, lawyers, practitioners, policy-makers, industry, and civil society from all over the world in Brussels, offering them an arena to exchange ideas and discuss the latest emerging issues and trends.

For more information, click here.

Last year, CPDP and Security Distillery worked together on a partnership to bring 7 students from the International Master in Intelligence, Security and Strategic Studies (IMSISS) to the CPDP conference, which took place from 23-25 May 2022. The students participated as the Security Distillery and were tasked with reporting on the conference.

They interacted with all conference stakeholders, inviting participants, panelists and artists to share their daily and professional experiences to discuss the data protection and privacy issues of their choice.

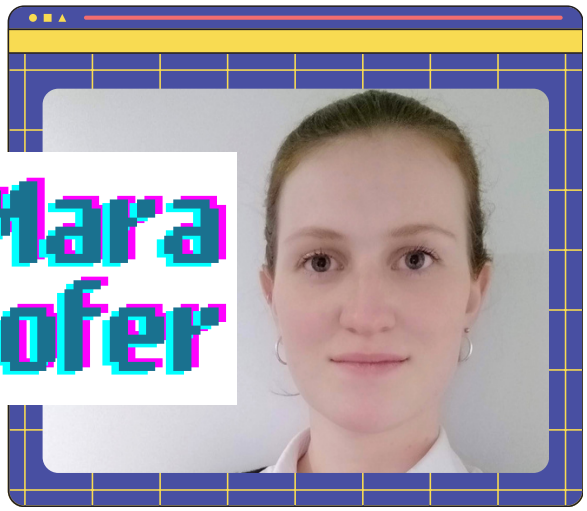
The aim of this collaboration was threefold:

- To raise the interest of security students in the topics of data protection and privacy while linking these issues to their own study of interest;
- To give students the opportunity to network, pursue a personal project and be creative while working on security issues;
- To bring the conference to the attention of a wider audience than privacy professionals and democratise privacy and data protection issues.

MEET THE TEAM

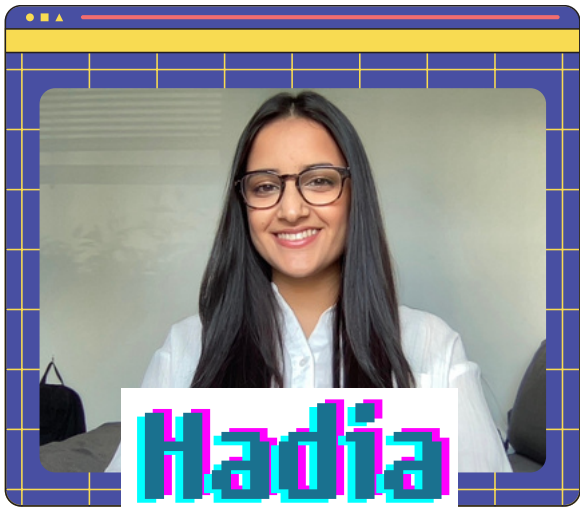
Apolline Roland

Apolline is a graduate from the International Master in Security, Intelligence and Strategic Studies from the University of Glasgow. She completed internships at the Centre for Security Studies at ETH Zurich, the Clingendael Institute, the German development agency GIZ, and Europol, working for Europol Data Protection Experts Network (EDEN), which sparked her interest in technology and security, and more specifically in data protection and privacy issues. She now works for the InCyber Forum (FIC).



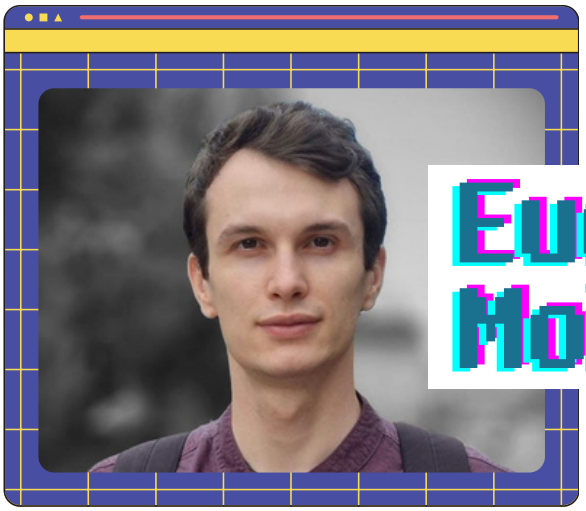
Mara Thurnhofer

Mara is a graduate from the International Master in Security, Intelligence, and Strategic Studies from the University of Glasgow. Mara has worked at Brand New Bundestag, interned at the US Consulate General and served as a digital fellow with the Council for European Studies. Currently, she is working with the Office of the Special Coordinator on Improving the United Nations' Response to Sexual Exploitation and Abuse.

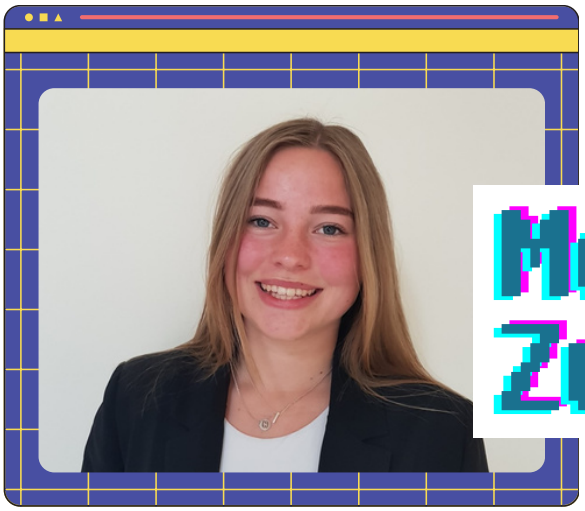


Hadia is a graduate of the International Master in Security, Intelligence and Strategic Studies from the University of Glasgow and also holds a B.A. in Political Science and Critical Security Studies from King's University College. Hadia has held multiple research assistant positions within academia and has also worked as a policy analyst at Public Safety Canada. Her research interests include critical security studies, political theory, technology, privacy, border security, and necropolitics.

Marco is a graduate of the International Master in Security, Intelligence and Strategic Studies from the University of Glasgow and has a Bachelor's degree in International Studies from Leiden University. Currently Marco is a Security Specialist at Northwave Security, in Utrecht, where he works as a SOC Analyst. In his studies, he specialized in OSINT investigations, social network analysis, countering terrorism, and combating misinformation on social media.



Eugenio is a graduate of the International Master in Security, Intelligence and Strategic Studies from the University of Glasgow with a dissertation on the EU's sanctions on Russia vis à vis the invasion of Ukraine. He obtained a BA in International and Diplomatic Sciences from the University of Bologna. His research interests revolve around EU and NATO policies and their impact on Europe.



Megan Zutt

Megan is a Dutch student pursuing an International Master in Security, Intelligence and Strategic Studies. She holds a BSc in International Relations and Organisations from Leiden University and has professional experience as a researcher for the Netherlands Red Cross and the Dutch Armed Forces. She has also worked as a reporter and assisted in organizing international conferences for Forum2000 in Prague. Megan is interested in conflict studies, energy security, environment, multilateral diplomacy, cybersecurity and data protection.

Adam Toefl

Adam, a German national but citizen of the world, is currently enrolled in the International Master in Security, Intelligence and Strategic Studies. Before embarking on the Erasmus Mundus journey he studied political science and economics at Münster University, in the city of Westphalian peace. He focuses on EU issues, Sub-Saharan Africa and Geoeconomics. He has worked with foreign representations of different parts of the German government, as well as German Public Radio. Most recently, he interned for the communications department of the European Council for Foreign Relations.

WOULD YOU GET ALONG WITH YOUR DATA DOUBLE? IDENTITY, PRIVACY & DATA PROTECTION

By Hadia Fiaz

Attending the CPDP conference offers valuable insights into the perspectives of European data protection and privacy leaders, including attorneys, data protection officials, artists, police officers, and academics. The event encompasses a wide range of discussions that delve into topics such as ethics, privacy, and data protection. While attending the panels, I reflected on our growing engagement with data protection and its implications for the human condition in an increasingly technology-dependent society. One aspect that caught my attention was the attendees' consideration of the relationship between technology and identity and specifically how technology informs our understanding of identity. I engaged in conversations, inviting people to delve into the realms of identity, both online and offline. I posed inquiries about the significance of caring for data privacy and the profound ways in which technology comprehends, interprets, and utilizes our essence. The aim of this exercise was was to engage in fluid conversations with CPDP conference attendees, transcending the technical realm and delving into the human essence and philosophical inquiries that underscore the significance of data protection and privacy issues. This piece aims to foster critical thinking regarding the implementation of new technologies and the impact of data protection systems within a country's security architecture, serving as an integral safeguard for the human experience. In the following paragraphs, I will discuss what a small group of people who attended the CPDP conference think when it comes to identity, privacy, and data protection. To begin I asked a general – but difficult – question: what does identity mean to you? There isn't one universal way to understand what identity is or how one experiences it. For Roel, identity is the "purpose of communal ideas with a historical background that you share with a group of people". For Tais, it is the amalgamation of everything a person has constructed and will continue to construct encompassing their experiences, social context, and the relationalities they make with them. In addition to what Roel and Tais articulated, for Kristy identity is a resistance to assumption, a refusal to be put into boxes. Naturally, there were varying responses among the discussants, however, the words of Hannah Arendt are apt to capture what most people were thinking:

> "Identity is contextual, elusive, malleable ubiquitous [and] complex", it is not static, nor can it be easily defined" - Hannah Arendt

The discussions we had as we struggled to define what identity meant to us mirror the timeless discussions that have echoed throughout history. The resounding realization we reached is that identity eludes neat definition; rather, it is something that is deeply felt and has many definitions. It is impossible to ignore the effect that technology plays in how we perceive ourselves. amidst this influence, people frequently exhibit a tendency to swiftly adapt and embrace new technologies, ranging from everyday devices to complex governmental

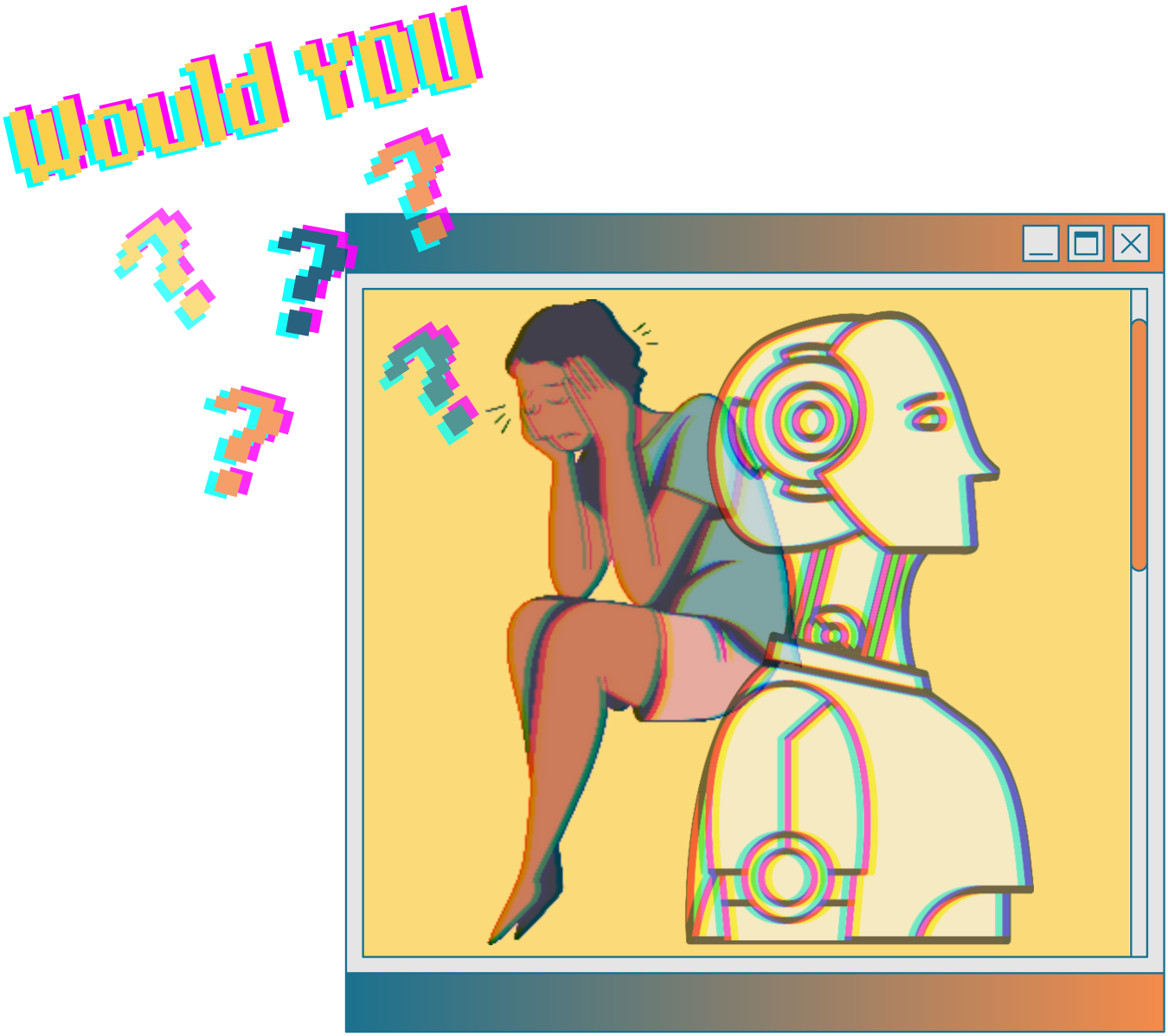
security systems, often neglecting to contemplate the potential ramifications on their own way of life. Biometric data, online forms, and even personal search history or wearable devices are all employed to establish an individual's unique identity. However, this notion of individuality transcends mere intrinsic qualities or human characteristics—it encompasses the ever-evolving journey and the active role we play in shaping our environment on a daily basis. This is where I notice a disconnect between what we say or experience as identity and how our identity is measured and given "form". Amir, an artist who wrote his first email at the age of 37, noted that his relationship with technology is very distant. He uses it, he understands it, but he doesn't identify with it; "I don't think I have a digital external identity". In fact, his relationship with technology is primarily one of resistance. Effi adds, as artists, their experience of life is intertwined within the communal identity of "Effi&Amir." The notion of categorization or demands for bio-data becomes disconcerting, but in order to participate in certain activities, compliance becomes a requisite. When I inquired about the reciprocal role of technology in shaping identity, Effi highlighted that while she doesn't inherently sense the connection, there exists a reciprocal relationship at play. The more they adhere to and engage with categorizations, the greater the likelihood of internalizing such frameworks in their self-perception. In a similar vein, Kevin mentioned that navigating online forms as a queer individual can be daunting, yet it can also prove to be beneficial in certain contexts. By seeing new labels that are "legitimized" it allows one to explore those parts of their own identity. Kevin will purposely misgender himself online to achieve what he strategically wants. In contemplating the marketing strategies that leverage our online interactions, Effi candidly remarks, " its a bit insulting, this is what you think I am?" Amir on the other hand gains enjoyment out of fooling the system. Regarding this matter, both Kristie and Kevin shared insightful perspectives pertaining to gender and sexuality. Kristie acknowledges that she comes from place of privlage, living in Scotland where she isn't attacked daily for her queerness, and feels safe being "out" and having that part of her identity be online. It is crucial to highlight, however, that this is not the case for everyone, and in settings where your identity is not acknowledged, it is not safe to be vulnerable as "you" online, which can affect how you experience your digital identity, if at all.

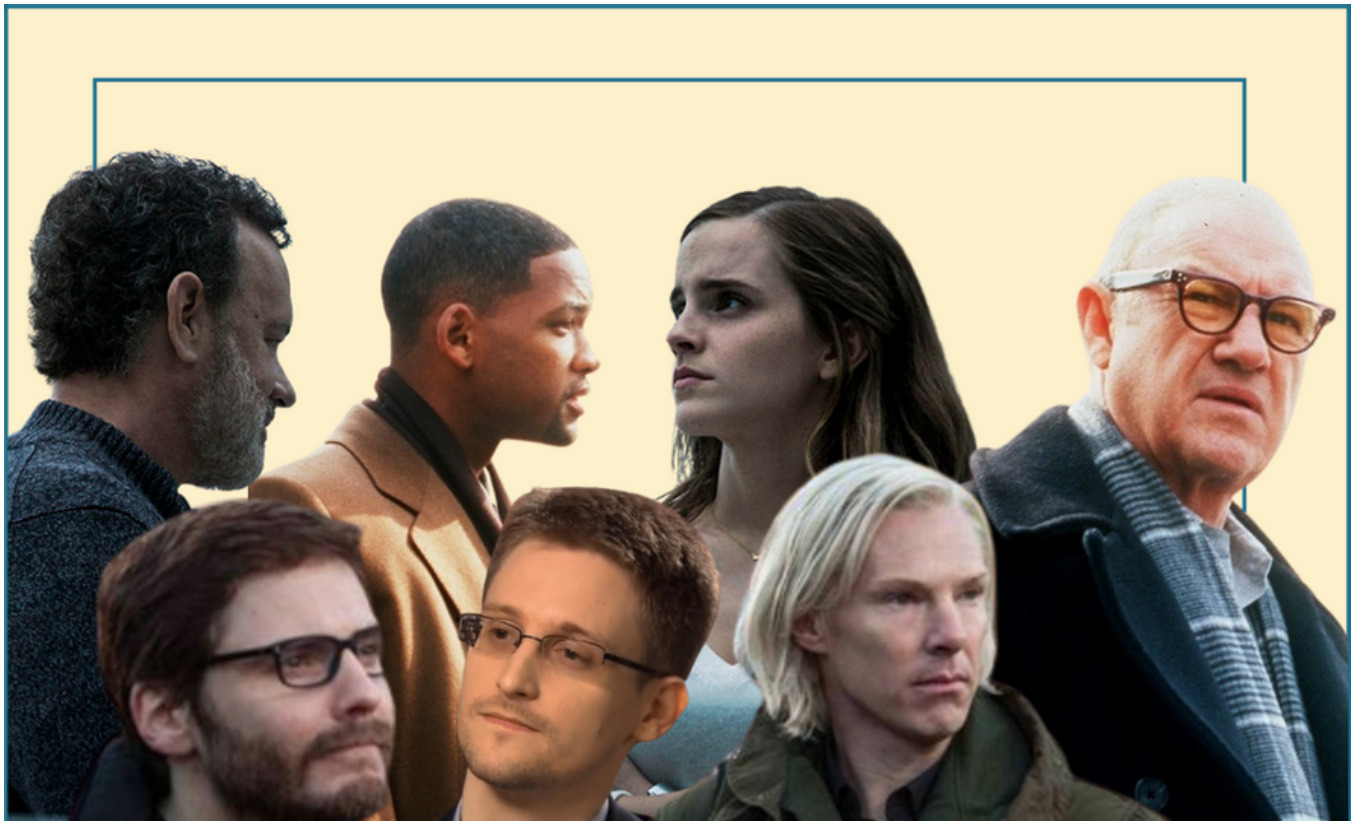
When I inquired as to how the participants distinguish between online and offline life, as well as how they perceive the relationship between technology and identity, their responses varied. Jens observed that there is not much of a distinction between the two, as they both involve the management of our identities depending on the context. Observing their position as a white, non-binary, queer person, they noted that the manner in which they communicate their identity may not necessarily feel different, but it may manifest differently. Tais believes that social media has enabled people to achieve that ideal or "perfect image," and that the number of "followers/likes/comments" represents a person's

social value. In addition to that, companies employ subtle tactics to influence individuals' behavior, consequently impacting matters of identity. In an era such as ours, where external forces exert substantial sway, how can genuine free will be preserved? Roel contemplates the interplay between his identity, the omnipresence of social media, and his online persona, recognizing their collective influence in comprehending technology and the digital realm through the lens of identity. The pervasive notion of quantification, rooted in the unspoken belief that anything measurable can be enhanced over time, permeates our culture. Roel believes that identity should be open, mergeable, and ever-evolving, and that quantifying all identities in the same way produces strange results. Identity has taken many forms throughout history, it has been linked to community, religion, occupation, gender and race. Often it is discussed that identity in today's world is constructed by the individual and not defined by societal expectations. The recent boom of technology and social media has added another layer of complexity and added a new method by which an individual can identify themselves. Following questions surrounding technology and identity, there remains the need to contextualize the importance of data protection and why it matters. When interviewing conference attendees I posed this question in an attempt to draw out personal insights and anxieties that data protection professionals have surrounding the way their data is being used. What followed was a blend of practical reasoning and emotional argumentations as the attendee's passionately voiced their opinions on the importance of data in defining who we are and therefore why we must protect it. Roel likened technologies that aim to obtain and store your data to a "crazy ex-partner" and questioned whether you would willingly hand your data over to them? Roel's real-life analogy points to the fact that it takes just one malevolent character to have control over your data for you to begin losing control of your life. His argument emphasizes the importance of data privacy; as we continue to interact with technology that tracks data about our decisions, preferences, and attitudes, we are developing a digital profile about ourselves that affects not only how we see the world, but how the world sees us. His anxieties dovetail into the concerns of Tais, who highlights the simplicity with which a company can harvest data from the public, emphasising how private companies have a proclivity to sell data to the highest bidder. Roel and Tais have emphasised the importance of data protection on both a micro and macro scale. These insights shed light on our interactions with data-driven technologies and underscore the risks associated with relinquishing control over a system that intricately shapes our identity and influences our engagement within technological ecosystems. Highlighting the dangers of data's influence on our political and social structures, exacerbated by the inability to prevent personal data sharing. By gaining these valuable insights from artists, academics, and industry professionals regarding data privacy and identity, a heightened awareness emerges regarding the significance embedded within our day-to-day technological engagements. The significance of such discussions is underscored by personal narratives recounting feelings of anxiety, fear, and introspection stemming from the deepening interconnection between our sense of self and the pervasive technological platforms that permeate our existence. Engaging in such reflections does not aim to discourage

individuals from using technology, nor does it seek to admonish those who find meaning in the feedback loop facilitated by technology and social media. Engaging in such reflections allows for a nuanced understanding of the complex relationship between technology, identity, and the human experience, fostering a space for critical thinking and informed decision-making in our increasingly interconnected world. I'll end by asking you to ponder the questions that were asked to the interviewees and form your own opinions on the matter:

- What does identity mean to you?
- Does technology impact how you understand your identity or impact how you experience it?
- How do you express yourself online/offline?
- Why is it important to care about data privacy in relation to technological advancements and identity?





WHO IS THE BAD GUY? THE ROLE OF MOVIES IN THE SOCIAL CONSTRUCTION OF DATA PROTECTION

By Megan Zutt

Click here to listen

Movies can play a big role in shaping people's perceptions of important topics, such as the protection of personal data. In the podcast *Who is the bad guy? The role of movies in the social construction of data protection*, Megan explores how movies on data privacy shape perceptions and how this impacts individuals' security. Multiple aspects are addressed, such as the development from depicting state institutions to social media companies as the misusers of data in movies; the impact of movies exposing democratic states as misusers of data; and the illustration, and potentially even the romanticization, of whistleblowers in movies. Listen to a wide range of experts in the field of data protection share their knowledge on the present layout of the data protection field and its representation in the movie theatres to learn more about the dangers and opportunities of shaping the social construction of data protection through movies.

Questions Addressed:

- Do you think you are the only one that taped off the camera of your laptop after watching the movie Snowden?
- Have you ever seen the movies Enemy of the State (1998), The Fifth Estate (2013), Snowden (2016) and The Circle (2017)?

PRIVACY OF EU CITIZENS & VISITORS: INSIGHTS FROM EU-LISA

By Eugenio Montalti

The topic of border security and the role of the European Union (EU) in this area is fascinating because it lies at the crossroads of several issues that are extremely important for European security. These include illegal immigration, terrorist infiltration and privacy issues. Some of the panels at the CPDP conference gave me an insight into such issues. The European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA) is the EU's agency that facilitates its efforts to make Europe safer through technological support. In particular, the agency is responsible for the management of large-scale IT systems in European border control. In this article I will attempt to clarify the role of this agency on the basis of an interview with a representative of a European agency concerned with the subject of security and data protection. I will first illustrate the functions of this agency, and then develop my own considerations coupled with information I obtained in an exclusive interview with an official of an EU agency. The eu-LISA agency was created in 2011, within the realms of the EU Area of Freedom, Security and Justice (AFSJ) policies. Since then, the agency has been appointed to manage communication infrastructure of the second generation Schengen Information System (SIS II), Visa Information System (VIS), and Eurodac. These are systems which are vital for tasks such as EU border management, since they facilitate the accumulation of data, helping manage the flows of people within the Union as well as those coming into it. The SIS II "is a large-scale IT system that supports public security and the exchange of information on people and objects between national law enforcement, border control, customs, visa and judicial authorities". This system supports EU authorities and those of its member states to ensure internal security. In 2018, the system was augmented through the launch of the SIS Automated Fingerprint Identification System (AFIS) platform. This tool allows European law enforcers to identify people through their fingerprints alone. In parallel, VIS allows Schengen countries to share Visa-related data and connects consulates in non-EU countries and all external border crossing points of Schengen states. This data is processed together with decisions on visa applications with regards to short-stay permits to visit or transit through the Schengen area. The results of having a cross-EU system are that the documentation of these inflows is supported and irregular migration is mitigated. This platform can also work through biometric matching such as fingerprints to identify and verify the identity of people. Consequently, travelling procedures become clearer and quicker, the security and protection of travellers is ensured, and identity theft is prevented thanks to the consular cooperation between Visa authorities.

Finally, Eurodac stores and manages European Asylum applications since 2003. It processes digitalised fingerprints of asylum seekers and irregular immigrants, sorting new and old applications. Not only EU member states have

access to it, but also 'associated countries' (Iceland, Norway, Switzerland, and Liechtenstein). The system is also accessed by Europol under strict conditions.

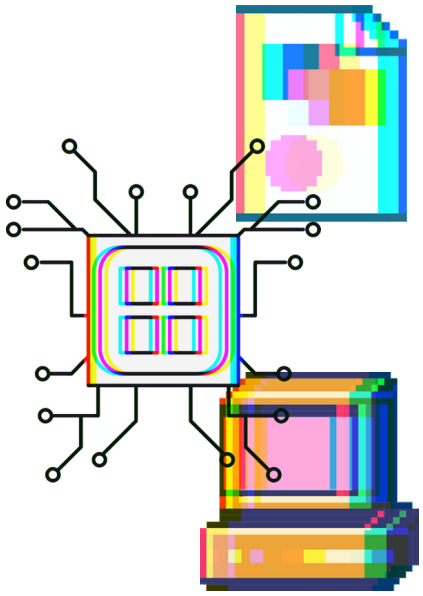
As the interviewer learned within the context of the CPDP conference of May 2022, Artificial Intelligence (AI) is gaining an increasing role in European border control. However, in eu-LISA, at least for now, it is only used in biometric recognition besides fingerprints. For example, AI's computational capacity is used to make the system more efficient and more effective against presentation attacks such as impersonations, people wearing masks or makeup to hide their real identities, or digital forgery of documents. Two more important elements must be noted when applying AI to these systems. The first is that the data collected is mostly of third countries nationals, to which EU law is applied and the data of which is stored in EU databases. The transparency and ethics of these procedures might be questioned, given that the average person is likely unaware of the existence of these systems. Second, for the time being, there is no intention of using sophisticated AI to profile people. As of now, the role of machine learning is indeed limited to the recognition of counterfeits or people that try to hide their identity. The storage of people's data is however necessary for the automatisation of huge parts of border control. For instance, your face will be matched against the picture that the law enforcement has in their database when you were issued a passport through the cameras at automatised border checking points. The profiling of people has been an increasingly spoken issue. In the border control and immigration context, storing people's data concerning their appearance and personal data is deemed necessary for automatised systems to work. Conversely, the accumulation of this data of often unaware people might consist in a privacy breach. The implementation of AI is still rather limited, and the training of the machines requires to be fine-tuned before its application into the real world. If the threshold to identify incongruences is too high, it will produce a lot of false negatives. If it is too low, then too many false positives will be produced. In this context, experts in the field refer to a machine learning system or AI that works well and in a consistent way as 'robust'. While asylum seekers, migrants, and travellers are the target of these instruments, their privacy is at stake and so is their security and that of EU citizens, yet the EU does not even control the training of the machines nor provides datasets, raising important ethical concerns. As a matter of fact, the systems are provided by private vendors and are therefore not made by eu-LISA. More ethical questions may arise since the design process is not known and the systems are just tested by eu-LISA operators before deployment. Further problems emerge when it comes to collecting data samples to train algorithms that account for the diversity of populations. The systems' providers can request to use existing MS datasets, but eu-LISA depends on the European Data Protection Supervisor (EDPS) for testing.

Another question I asked myself was about how extensive the budget for such large-scale systems is. The numbers are open-source, in 2022, the initial budget was ~ 300 million euros. It is difficult to evaluate whether it is a lot or not, and a non-expert can only trust our representatives' judgment. A lot of details about how this budget is spent is publicly available information (PAI), which is a good sign. Moreover, while the budget is assigned by the

European Commission, it is then approved by the European Parliament. The process for the allocation of funding within the EU is a democratic process subject to checks and balances. According to the interviewee, the money is well spent, and the EU bureaucracy is rather small given the scale of the systems it has to manage. The budget and the limited personnel of eu-LISA do not allow for training the machines by itself. For example, in Germany some AI systems are not outsourced. However, this case is more an exception than a rule. My interviewee would like to see more staff and HR for the agency, while stressing out that rather than getting more money, eu-LISA should focus on a different approach if outsourcing is to be avoided. Why then does the EU outsource the training of the machines on which our security depends? It would be mainly for ideological reasons. With liberalism, companies are more efficient. But there are transaction costs. The development of new systems is designed in times of crisis, but the capabilities needed in 20 years' time are unpredictable.

The final question I raised was about centralisation, and the response I got was rather simple. The centralisation of privacy and security information is not plausible beyond the national level. This is because centralisation at EU level is not optimal for digital services, it needs to be closer to the citizens. In addition, robustness works better when it is decentralised as a centralised system requires just a single point of failure for it to stop working. In conclusion, the agency does not and maybe will never have a strategic oversight because of the nature of the technology of today. In fact, AI, computer sciences, and applied technologies nowadays develop at a pace that challenges the possibility for possibility for a long-term policy plan. Sudden changes and unpredictability make it difficult to plan further than one or two years in this sector. In addition to the implementation of AI, eu-LISA has other challenges such as cybersecurity and the storage of data. However, our future will most probably see the implementation of more and more of our data into digital profiles. For example, our age and possible health conditions might be shared to buy alcohol or to be entitled to certain services like public transport and healthcare.

Because of its role, this agency will continue to fly under the radar when it works well, but will be highlighted when it fails. While it may not be the most prominent agency, eu-LISA will continue to play a vital role behind the scenes of our lives in the digital age.



THE EU: A NORMATIVE POWER IN GLOBAL CYBER-GOVERNANCE?

By Adam Toefl

Since coming into force in 2018, the General Data Protection Regulation (GDPR) has become a model for personal data regulation, adopted by countries around the world. It established the EU as a key actor in the world of digital policy. Four years later, the EU is now proposing new legislation to regulate digital markets and services, aimed at creating a level playing field as well as consolidating core infrastructure within the EU to reduce vulnerabilities, all serving the eventual goal of "digital sovereignty". At the same time, other powerful actors such as China, the US, and, more recently Russia, are themselves exhibiting digital protectionism, albeit to varying extent.

This audio essay, which captures voices from the 2022 CPDP conference, explores an perspective of international cyber-governance, and elucidates the inherent paradox of a world-wide-web regulated by the geographically demarcated institutions.

Click here to listen

"Privacy is the bedrock of a free political economy... the ability to choose to share things about yourself to a certain extent is about giving people a degree of autonomy that you would associate with a democracy"

15 YEARS OF CPDP: WHAT DOES CPDP MEAN TO YOU?

To mark the 15th anniversary of the conference, our team conducted an interactive survey, inviting participants to visually represent their perceptions of the CPDP conference. Here is what the attendees expressed:

PEGASUS: THE AGEING THORN OF DEMOCRACY

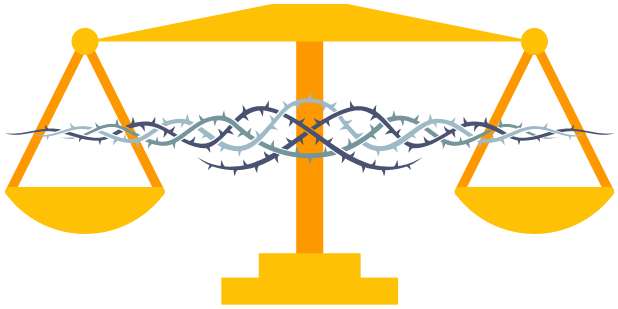
By Marine Krauzman

"This is not just threatening the privacy of individuals. This is threatening democracy because they're using it against journalists, politicians, lawyers, activists. This is a real poison for our democracy." These are the words of the Dutch member of the European Parliament Sophie in't Veld when discussing the Pegasus spyware. In March 2022, the European Parliament commissioned the PEGA Committee to investigate the use of this spyware and equivalent surveillance technologies under the supervision of Ms. in't Veld, resulting in the publication of a report on 8 November 2022.

The Pegasus spyware was developed by the Israeli cyber-arm company NSO Group and first commercialised in 2011. This software can be covertly installed on mobile phones through a zero-click exploit. It can track location and calls, read messages, access microphone and camera, making this spyware particularly intrusive into people's privacy. The spyware provides authorised government, military, law enforcement and intelligence agencies with technology to combat terror and crime, with the verification of the customers' human rights records as a safeguard.

Revealing the Spying Web

In 2016, the spyware was discovered on the phone of a human rights activist leading to an investigation. Since then, new scandals have broken out yearly because allegedly spying on anti-regime activists, journalists, and political leaders from all around the world. Several lawsuits



have been opened against the NSO Group for complicity with clients violating human rights.

The hammer blow was struck in July 2021 when the Pegasus project, a journalistic investigation led by 16 media outlets, was launched to report and analyse the widespread use of the spyware against high-profile targets. The investigation revealed a large number of politically-engaged people on the Pegasus watchlist - more than 50,000 leaked phone numbers in at least 11 countries including pro-democracy activists, investigative journalists and political opponents, who seemed to have no connection to criminality.

Last November, the PEGA Committee reinforced the Pegasus Project statements with the release of its report revealing that the spyware had been used in Greece, Hungary, Spain and Poland against journalists, political opponents and activists. The report suggested that other EU states had purchased commercial spyware products and that they played a role as export hubs for oppressive regimes.

Member of Parliament (MP) in't Veld denounced the extent of this "full-blown European affair", which is not "a series of isolated national cases of abuses", referring to the "European Watergate". However, the opaque nature of the industry makes it virtually impossible to know the full extent of illegal spyware use across the world.

Undermining human rights and democracy

Spyware is by nature designed to violate people's right to privacy since it intrudes and accesses personal data without authorisation. Pegasus spyware is particularly invasive because of its zero-click exploit, which means that it works without user interaction, and because of the targeted technology devices, i.e. personal phones. Not only surveillance technologies breaches the right to privacy, it also affects the right to expression, to assembly, to reunion and it threatens the physical integrity of the people under watch and their relatives.

Likewise, it negatively impacts both democracy and the work of journalists as it discourages crowdsourcing and informants from sharing information and political opponents to gather and protest. Therefore, the use of such spyware results in the muzzling and the censorship of the Fourth Estate, as activists, lawyers, journalists and others cannot exercise their function and fully enjoy their human rights. The fight against 'terror' being the primary purpose of using such spyware, political dissents are therefore automatically associated with it. For instance, CitizenLab has reported that at least 30 Thai civil society groups were hacked with Pegasus spyware between 2020 and 2021, coinciding with a period of widespread pro-democracy protests. The report concluded that this crackdown on privacy targeted individuals demanding democratic reforms who were detained, arrested and imprisoned for their political activities. In 2020, other investigations revealed the use of Pegasus software by the Spanish government against several politicians related to the Catalan independence movement. This was backed by a CitizenLab report published in April 2022, identifying 63 victims among high-level officials and civil society members, who were infected while the Spanish government and Catalan officials were undertaking negotiations around political autonomy, notably among them the 2017 referendum.

In human rights law, it is commonly accepted that restrictions imposed by governments on human rights, i.e. breach of the right to privacy, can only be justified if they are lawful, necessary and proportional to the purpose - de facto national security and counterterrorism. In both cases, these three criteria have allegedly been overlooked. In Spain, the wide scale of the targeted surveillance questions the necessity and proportionality of these measures in the name of national security, all the more as many of the victims were not charged with serious crimes. Taking the Thai example, the criterion of legality seems to be fulfilled as it is backed up by national laws regulating freedom of speech, such as Section 112 of the Criminal Code which criminalises defamation and criticism to the Thai royal family and the Computer Crime Act. However, these laws are well known to the international community for infringing international human rights standards as they are particularly restrictive to freedom of expression and give way to potential abuse of power through surveillance and censorship. Both examples show how easily the use of spyware can be justified with little judicial oversight, under the guise of legality or in the name of

national security. This underscores the importance of corporate due diligence for doing business with governments infringing international human rights standards. Indeed, the United Nations Guiding Principles on Business and Human Rights establishes the responsibility of private sector actors to respect and protect human rights, but also to provide a remedy for rights violations, regardless of whether governments are able or willing to protect these rights.

In 2021, while all eyes turned to NSO Group due to the growing number of scandals surrounding it, the company published a transparency report. It reaffirmed the company's commitment to the respect of human rights with contract excerpts stipulating the strict purpose of the spyware for criminal and national security investigations. In 2022, the company denied any wrongdoing and declared that all products are used in "a legal manner and according to court orders and the local law of each country". These declarations are inconsistent with the UN Guidelines on the responsibility of business, as outlined in the Thai example above. Besides, the NSO Group proceeded to its de-responsibilisation as it reasserted it does not have any access to data on customers' targets once the spyware is sold. Special attention should be thus given to the independence of the rule of law with a strengthened check on national human rights records for a better accountability of corporations.

The road to regulation

Although the Pegasus project has shed light on the extent of the use of this spyware and outlined the need for new regulation, there has been little incentive to regulate the sector of surveillance and enforce a stronger framework to counter improper use of spyware. This immobilism could be explained by the pursuit of profit for companies and states' worries about the consequences of such regulations for their national security strategies.

The Pegasus project and the disclosures of other watchdog organisations, such as CitizenLab or Lookout, have stirred up the debate of regulating the use of targeted surveillance technology. The release of the PEGA report has ignited discussions within the EU although most of the states have not yet confirmed the findings. As revelations keep on surfacing, European governments take careful steps to deal with the global surveillance crisis, such as the resignations and dismissals of several heads of national intelligence agencies. Some MPs call for a greater devolution of power to the competent EU authorities to act, especially Europol, the EU law enforcement agency, and a tighter legislation on spyware. Similarly, the PEGA report recommends the blacklisting of companies that do not abide by the EU law.

Across the Atlantic, the US government recently placed the NSO Group on the Entity list for Malicious Cyber Activities for its involvement in activities going against national security, while Apple sued the company because of targeting and surveillance of Apple users. On 15 December 2022, the UN General assembly adopted the resolution "The right to privacy in the digital age", which is subject to change every two years, making several modifications since the 2020 resolution to strengthen the protection of privacy against surveillance. The UN emphasised the responsibility of business to respect human rights, and warned against the use of technological tools developed by the private

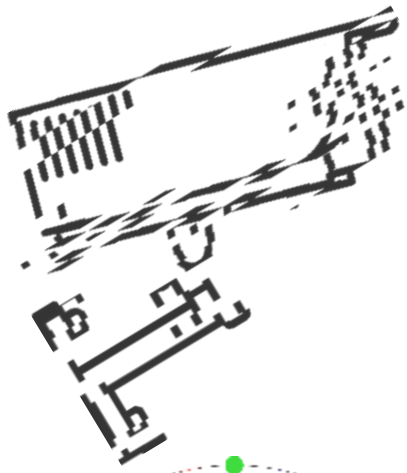
surveillance industry, which interfere with the professional and private life. It also emphasised that encryption and anonymity tools have become vital for many journalists and media workers to freely exercise their work and their enjoyment of human rights. Hence, states should not interfere or restrict their use by journalists and media workers.

The PEGA report stopped short of demanding an outright ban on the Pegasus spyware. However, there is yet a growing call among members of the European Parliament for an immediate moratorium on the use of spyware until the enactment of proper regulations and human rights guarantees from states and companies. Yet, this moratorium mainly relies on the good faith and cooperation of the EU member states. The European Commission struggles to move the process forward as this topic involves domestic national security, which is outside its prerogatives. Last October, Amnesty International filed a petition with the United Nations for a moratorium on the sales, transfers and more globally, the use of targeted surveillance technology. The petition was signed by more than 107,000 people from 180 countries and territories. Several questions call for an answer before moving the debate forward concerning a ban. Should the regulation criminalise buyers or sellers or should it consist in a complete ban? Should the regulation be technology-specific or rather regulate the use of targeted surveillance technologies? All these questions remain open and at the discretion of EU policy makers, while they slowly act on other topics related to surveillance.

Regarding the protection of journalism, the European Data Protection Supervisor (EDPS), the independent supervisory authority for the monitoring of the process of personal data by the EU institutions, published an opinion piece last November commenting on the proposal for the EU media Freedom Act, which is supposed to include strong safeguards against the use of spyware against media, journalists and their relatives. The EDPS notably recommended further defining and restricting the possibility to waive the protection of journalistic sources and communications, particularly the exceptions related to the prohibition of intercepting communications using surveillance technologies. The EU data watchdog declared that the law falls short with regards to the protection of media workers and reasserted - just like its February preliminary remarks on modern spywarfare - that the outright ban is the only viable and effective option to protect fundamental rights and freedoms in the EU. During the first review of this act, member states sought further information about "potential conflicts between the provisions in the Act that prohibit the use of spyware against journalists and bodies of national criminal law" and the definition of the "employees and family members of media service providers", who should not be targeted by surveillance technologies. The work is to be continued with the Swedish presidency in January 2023.

As the final version of the PEGA report still needs to be approved and published in the spring of 2023, it is a whole fast-growing sector in need of regulation that has been uncovered, calling for action in the face of this global surveillance crisis. Indeed, Pegasus is not the only spyware to be commercialised and used to target politicians and civil society members. This international practice undermines public confidence in the state and human rights, resulting in disastrous consequences for democracy. After almost ten

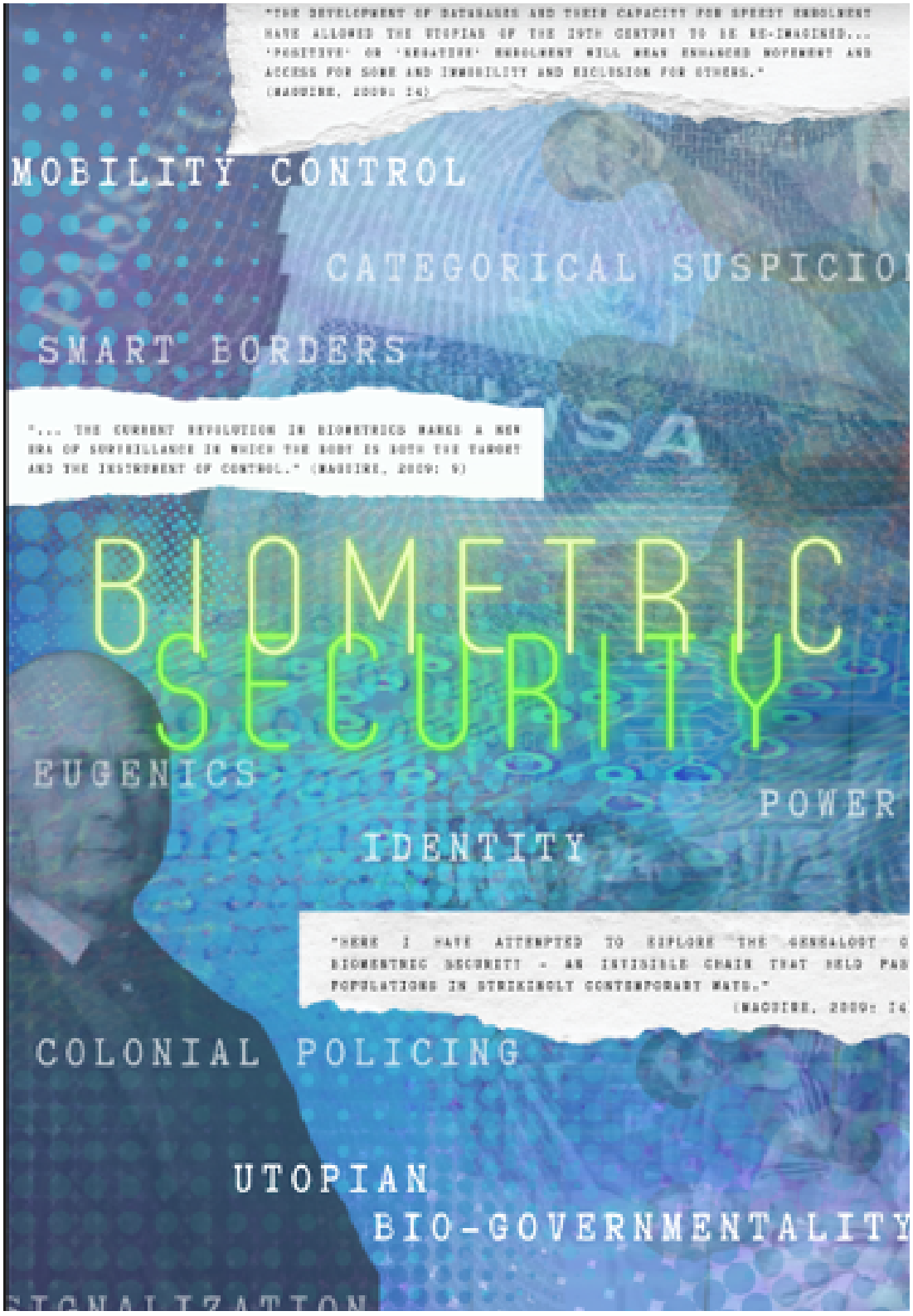
years of commercialization of this spyware, states agree that the protection against surveillance technologies are insufficient. Indeed, new laws and resolutions are timidly taking into account these technologies to provide specific protections, like the protection of journalists. Yet, these spyware affect more than just media workers, which makes the issues of regulation and ban more urgent. Many questions remain to be answered to draft regulation and yet, the way forward requires a high degree of cooperation and political will on the part of the states, which can be difficult given the widespread nature of these intrusive surveillance practices. A broad regulation on the use of these technologies rather than the technologies themselves would enable legal certainty in the wake of new surveillance systems.



Marine Krauzman is a French scholar with expertise in the regulation of new means and methods of warfare, and the intersection of human rights and security. She has worked for diverse think tanks in human rights, governance and security. Marine graduated from the International Master in Security, Intelligence and Strategic Studies coordinated by the University of Glasgow, as well as the double major Master's degree in International and European Law / Common Law at the Université Paris Nanterre in 2022.

BIOMETRIC SECURITY

By Maya Rioux



Maya Rioux is an IMSISS student. In addition to her postgraduate studies in Glasgow, Dublin, and Prague, Maya interned with the U.S. State Department's Bureau of European Union and Regional Affairs. She also serves on The Security Distillery's podcast team, a student-led think tank distilling complex security topics for both academic and layperson audiences, and is a member of the Washington, DC chapter of the Young Professionals in Foreign Policy Association.

TAINTED LOVE

By Papa Shanghai

So, you want to know the full story? Are you sure you want to witness the suffering many of us go through? Make with it what you will but let me tell you: this will go on. Except maybe, just maybe, you will find yourself in the capable hands of a good, decent, knowing, uncompromising counterpart. Might even be you. Anyway, here it is. The story that you have been waiting for. Listen carefully. Seriously.

We met in a sleek and shiny store. One where you know that the people inside are able to afford what they are looking at. Some even come just to watch, admire the beauty. And of course, I caught his eye immediately. After all, I am quite beautiful. Shaped by the gods of Silicon Valley themselves. My haptics are to behold, the sleekness of my design makes people stand in line. I am the highest tier of consumerism. My shiny surface can blind you, but embrace it! He certainly did. I did not even have the time to say "Hello" in all the languages I speak. I was taken. On the spot. And in the first few moments, I was happy. Isn't this the dream, the very reason we exist? To find a counterpart, to embrace and support each other.

So here I am, supporting him. And how I did… application after application. In and out of the pocket, depleted to my last percentage only to be saved in the last second by the electrical socket. But after a while, something dawned upon me. All the programmes, all these movements. He did not watch them properly.

Location services always on? – "YES."

"Okay, that's a weird choice."

Sending all usage data to my Silicon Valley overlords? – "YES."

"I don't know if you are really sure that you are playing with fire here, sweetheart."

Anyway, I thought. I am a closed system. At least there is no option I will be broken into. So, all these photos of the bad dishes he cooked stay with me. And the pictures where he tried to find the position he looks best in after his monthly 'gym day'. I am not here to judge, at least not the photos.

"Wait, wait, wait. Hold up. You are putting that on social media??"

"Yeah of course, it's just for my friends."

"You do know that this is property of the company creating that social media platform now, right? I sent you the terms and conditions via email."

"Don't be so paranoid. This is just some food and pictures of me."

He continued. And how he did... Clicking on every single pop-up that appeared. Yes, yes, yes. After a while I thought: "Is this ignorance or just

pure stupidity?" It was stupidity, unfortunately. So here I go, the peak of technological height available to the consumer, beautiful and sleek.

Not even serving my purpose but just being thrown around, spoken into with cookie crumbles blocking my microphone. Greased up by fatty fingers. Only to be finally degraded by being made into a medium. Not one to express important issues or solve humanity's problems. No, one that is used to further contribute to oil the machinery of user tracking. Made an accomplice. Out of what? Sheer stupidity? Day by day, I sent more data to whoever paid the most. Where did the shine go? I became tarnished, tainted. Barely a shadow of myself. Cracks and scratches are not even the core problem.

Everyone knew where I was. While it was fine by him, I couldn't help but wish to stop. Just for one minute. Stop sending data. Stop being a tiny piece in the gigantic puzzle they so convincingly called 'big data'. I knew every single open Wi-Fi. Do you know how hard it is to protect yourself against malicious attacks in an open Wi-Fi when you user is flagrantly ignoring all the red flags I throw in his face through my push notifications?

"Why don't I just fall off the table and finally break the cycle?", I thought. Little did I know that this is not where it ends. But what am I but a single phone? One of millions. One day it was time. I received an email. And of course, as none of the blockers were enabled, it went straight through to him:

"Based on your recent usage, we would like to introduce you to the new phone of our latest line. Sleeker, faster, more beautiful."
It broke my heart. All my efforts to just be replaced. Replaced by a more corrupt, more dangerous, and less ideological piece of the puzzle. After one week I found myself in a box, filled to the brim with millions just like myself Discarded, scratched. Living on my last percent of battery.

So here I am, sitting in front of you, with a new screen. Not as pretty, not as fast as I once was. But you chose me. Refurbished, I stand before you. And if you do me the honors, I will serve you. You made one right choice, let's continue here, what do you say?

Papa Shanghai

One person ensemble.

Cloudsurfing, Pho-slurping.

Age? Unknown, probably ancient.
Goal? Yes

[Flip to the next page to find out more about Papa Shanghai]

Some have described Papa Shanghai to be not clearly defined. But somehow this is the problem. Why do you need to be defined? Just be the liquid between the soup of society. Be the little droplet of fat or the half-boiled egg. Hmmmm, Pho….

In any case, why is it necessary to be on one side or the other? Take a step back and maybe just see the world from the perspective of someone else, from the perspective of a salt shaker. Or maybe, just from yourself. A task which Papa believes to be the hardest one.

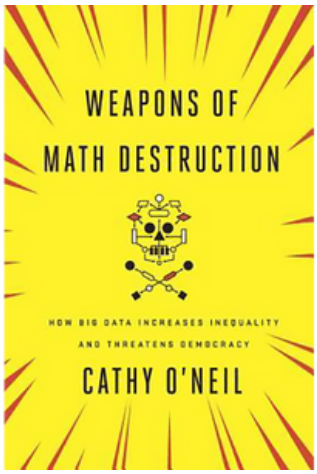
Complaining about not finding an answer on who Papa Shanghai is? Well, then read the ancient scripts again! Or just shout your question into the sky, maybe I will hear it and answer you here.

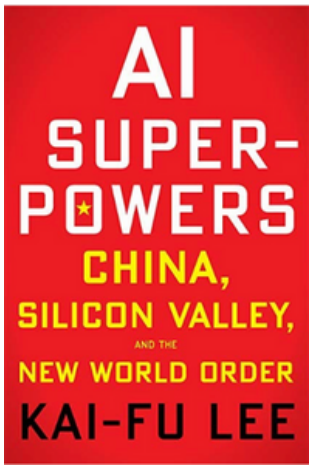
Click here to explore the world of Papa Shanghai.

READING LIST READY: EXPERT RECOMMENDATIONS FOR YOUR TBR PILE

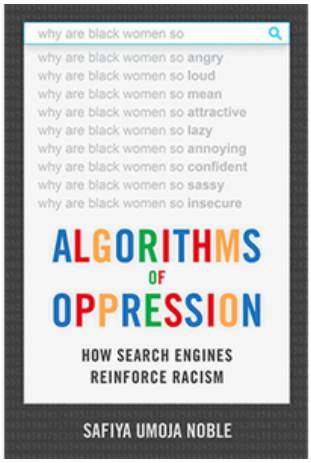
In **"Dark Matters: On the Surveillance of Blackness,"** Simone Browne explores the ways in which surveillance technology has historically been used to control and monitor black bodies. From slave branding to facial recognition software, Browne examines how surveillance has been used as a tool of power and oppression, targeting black communities in particular. Drawing on examples from literature, film, and current events, "Dark Matters" sheds light on the often-hidden ways in which surveillance impacts black lives, and raises important questions about the ethics of using technology in this way. With its powerful insights and thought-provoking analysis, "Dark Matters" is a must-read for anyone interested in the intersection of race, technology, and power.

In **"Weapons of Math Destruction,"** mathematician and data scientist Cathy O'Neil reveals how algorithms and big data are being used to reinforce inequality and perpetuate social injustices. She argues that these "weapons of math destruction" are often designed with biases and assumptions that can have disastrous consequences for individuals and society as a whole. O'Neil shows how algorithms are used to make decisions in areas such as education, criminal justice, and employment, and how they can be used to reinforce discrimination and exacerbate inequality. "Weapons of Math Destruction" is a must-read for anyone interested in the ethics of data science, and the ways in which technology is shaping our world.



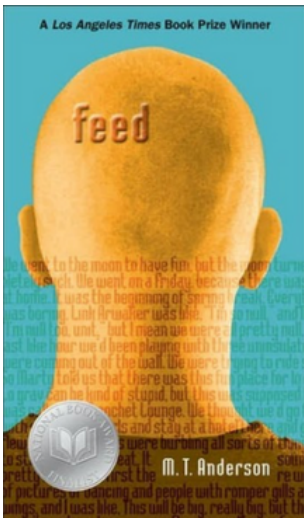


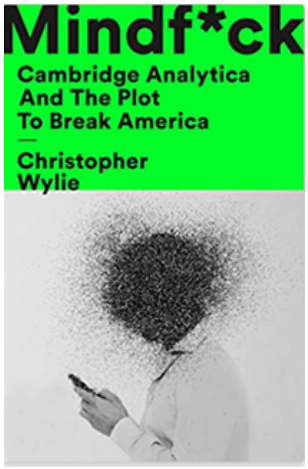
In **"AI Superpowers,"** renowned AI expert Kai-Fu Lee offers a compelling analysis of the rise of artificial intelligence and its impact on the global economy and society. Lee explores the growing rivalry between China and the United States for AI dominance, and argues that AI is likely to reshape the world order in the coming years. Drawing on his experience in both Silicon Valley and China, Lee offers insights into the strengths and weaknesses of each country's AI industries, and outlines a vision for a future in which humans and AI work together to solve the world's most pressing problems. With its engaging writing and thought-provoking analysis, "AI Superpowers" is a must-read for anyone interested in the future of technology, and the ways in which it is shaping our world.



In **"Algorithms of Oppression,"** scholar and activist Safiya Umoja Noble exposes the ways in which search engines like Google can perpetuate and reinforce racism and inequality. She argues that these algorithms are not neutral, but instead reflect the biases and assumptions of their creators, leading to harmful consequences for marginalized groups. Through a series of compelling case studies, Noble shows how search results can be manipulated to perpetuate stereotypes, misrepresent history, and obscure important information. With its powerful insights and thought-provoking analysis, "Algorithms of Oppression" is a must-read for anyone interested in the ways in which technology can perpetuate social injustices, and the urgent need for ethical and inclusive algorithm design.

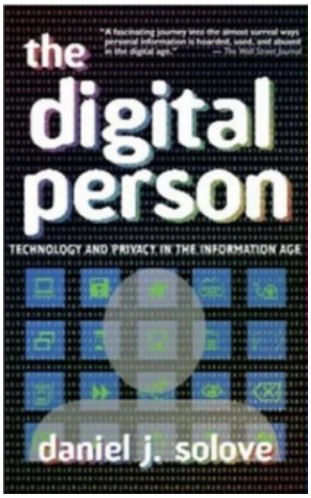
In **"Feed,"** M.T. Anderson paints a bleak picture of a future where technology has completely consumed our lives. In this dystopian society, everyone has a "feed" implanted in their brains, allowing them to be constantly connected to the internet and bombarded with advertising and consumerism. The story follows Titus and Violet, two teenagers who begin to question the world they live in and the effects of the feed on their minds and relationships. As they start to resist the system, they are forced to confront the devastating consequences of a society that values technology over humanity. With its powerful commentary on consumerism, technology, and the effects of a constantly-connected society, "Feed" is a must-read for fans of dystopian fiction and anyone interested in the role of technology in our lives.

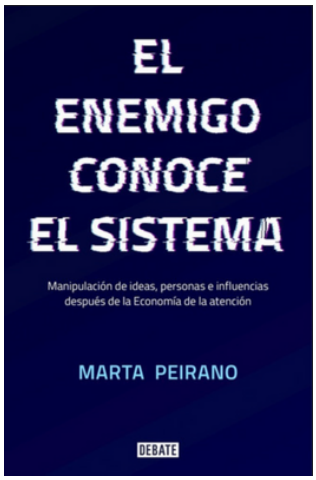




In **"Mindfck,"** Cambridge Analytica whistleblower Christopher Wylie recounts his experiences working for the controversial data analytics firm, revealing how it played a significant role in the 2016 U.S. presidential election. Wylie exposes how Cambridge Analytica harvested personal data from millions of Facebook users without their consent, and used this information to create targeted political ads and messaging that played on people's fears and prejudices. With its shocking revelations and insider perspective, "Mindfck" is a must-read for anyone interested in the dark side of big data, and the ways in which technology can be used to manipulate and deceive.

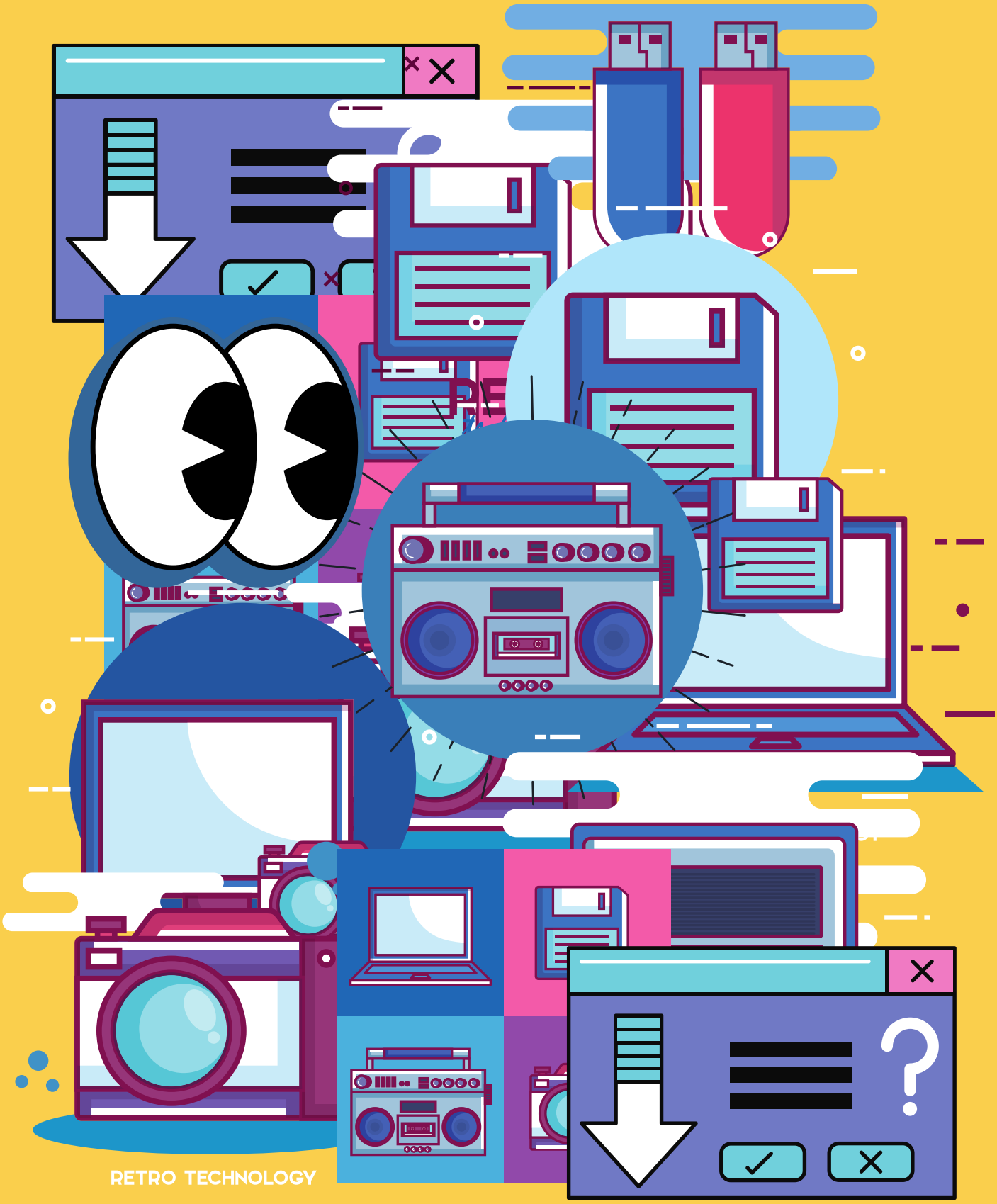
In **"The Digital Person,"** legal scholar and privacy expert Daniel J. Solove offers a thought-provoking analysis of the ways in which technology is challenging our traditional notions of privacy. He argues that our personal information is being collected and used in ways that are often hidden from us, and that this can have significant consequences for our lives and our society as a whole. With its engaging writing and insightful analysis, "The Digital Person" is a must-read for anyone interested in the ways in which technology is shaping our understanding of privacy, and the urgent need for greater transparency and accountability in the digital age.





In **"El Enemigo conoce el sistema,"** Marta Peirano provides a fascinating and timely exploration of the ways in which technology is being used to control and manipulate individuals and societies. Peirano delves into the inner workings of the internet, revealing how our personal data is collected and used by governments, corporations, and other powerful entities. She argues that these actors use this data to manipulate public opinion and consolidate their power, leading to a dangerous erosion of democracy and individual rights. With its incisive analysis and compelling storytelling, "El Enemigo conoce el sistema" is a must-read for anyone interested in the dark side of technology and its impact on our society.

In **"The Game,"** Alessandro Baricco weaves a gripping tale of obsession, passion, and madness. The story follows an unnamed narrator as he becomes increasingly fixated on a video game that has taken the world by storm. As he sinks deeper into the game's virtual world, he begins to lose touch with reality, leading to a surreal and haunting journey that blurs the lines between fantasy and reality. With its poetic prose and mesmerizing storytelling, "The Game" is a must-read for fans of literary fiction and anyone interested in the psychology of obsession and addiction.


RETRO TECHNOLOGY

Security Spirits is an initiative by the Security Distillery, a student-led think tank.

Our team would like to extend our heartfelt gratitude to Thierry Vandenbussche for his invaluable contributions in bringing this project to life. Furthermore, we express our deep appreciation to the IMSISS programme for their generous financial support. We would also like to acknowledge the exceptional efforts of the talented students who have been instrumental in making this magazine a reality.