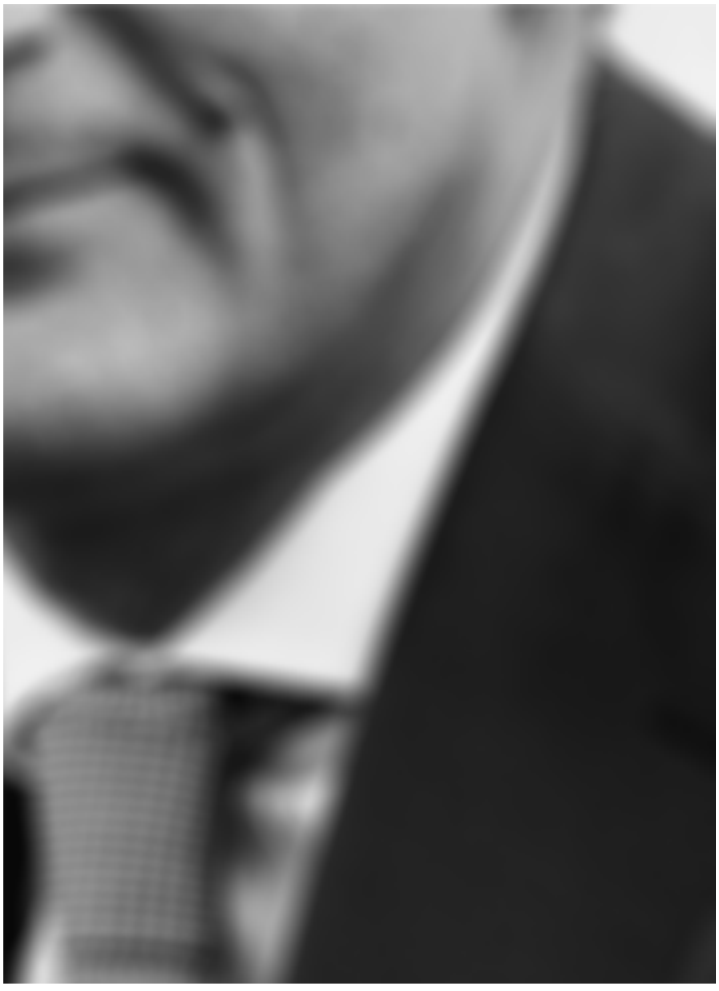
PRIVACY 2030

A New Vision for Europe

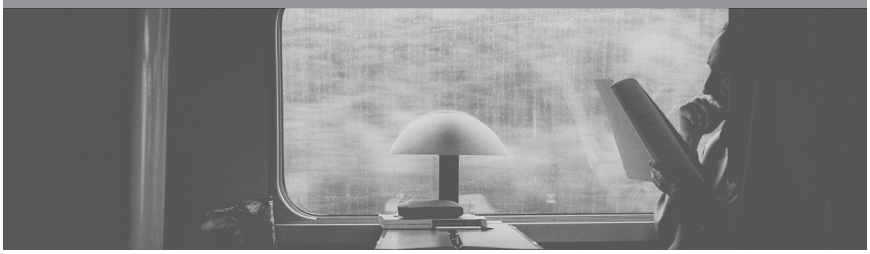


CONTENT

Introduction:

CARRYING BUTTARELLI'S TORCH

Omer Tene



In an age of algorithmic decision-making systems for criminal sentencing and driverless cars, Giovanni Buttarelli — beyond everything, a humanist — tried to put humans back in the driver's seat. While not dogmatic or doctrinaire, he watched with concern and skepticism as technologies that initially heralded a new age of borderless connectivity, frictionless sharing and rational choice took a dark turn toward the current crisis of trust, opaque systems and "fake news." He derided the "techno-solutionism" that saw society's railway engine detach from the passenger cars of the train, promising unfathomable riches and technologically assisted utopias for a fortunate few while at the same time condemning large populations to arbitrariness, commodification and manipulation. Somber and wistful, though with a constant glimmer in his eye, he spent his last days conveying his vision, his manifesto, to his friend, colleague and ally, Christian D'Cunha, who now shares it with the community.

An Italian in Brussels, Buttarelli had an intuitive grasp for and deep understanding of Machiavellian power struggles. Very early on, he foresaw how the aggregation of data in the hands of a few corporations would lead to an unconscionable accumulation of power. He recognized that beyond data protection, competition law and antitrust would emerge as necessary policy tools to address the excesses of the technology industry. Years before the recent decision of the Bundeskartellamt in the case of Facebook on the intersection of privacy and competition, the European Data Protection Supervisor wrote, "The interface between competition and privacy should be a central, strategic and long-term concern for all independent data

protection authorities." In his manifesto, Buttarelli warns against the creation of regulatory silos that would favor technocratic frameworks over a comprehensive view of the effects of data on the economy, society and even the environment. For him, it was always "privacy and..." — privacy and national security (when discussing the Schengen accords), privacy and competition (when considering corporate power), and most recently privacy and ethics (when considering big data and artificial intelligence).

A European through and through, Buttarelli appreciated the special role the EU has in setting policy for a digital age. Haunted by a recent past of totalitarianism and outbursts of savage conflict, Europe has been circumspect when facing an American climate of data-driven technological rapture, remembering that privacy is a bulwark against overreach by the state. To be sure, Europe's economy has been lagging compared to the surging growth in the U.S., not to mention China, its main technologically driven competitor. But as China erects a techno-driven totalitarian dystopia, and the U.S. sees platform architecture and cyber vulnerabilities present ominous threats to the very core of its democracy, including election interference and the splintering of public discourse into insular echo chambers poisoned by fake content, Europe has held on dearly to its notion of privacy and data protection as fundamental human rights. Importantly, Europe has successfully exported this vision, now buttressed by the Treaty of Libson and jurisprudence of the Strasbourg high court, to countries and regions across the world, from Brazil and Colombia through Sub-Saharan Africa to India and the Philippines.

Tall in spirit and stature, Buttarelli could always see beyond the next curve. His prescient vision of the role of digital ethics beyond the law and in the shadow of the law, a normative magna carta for a digital age, undergirds the European current strategy on AI. His appointment in 2015 of an Ethics Advisory Group and report "Toward a New Digital Ethics" foresaw today's policy debate about the appointment of organizational ethical review boards to assess the beneficence, equity and justice of automated systems and algorithmic decision making. The first conclusion of the Ethics Advisory Group, "The dignity of the person remains inviolable in the digital age," neatly conveys Buttarelli's conviction that regardless of the brilliance of airplane-flying, chess-winning, medical-condition-diagnosing machines, humans must remain at the helm.

Himself a part of Europe's elite, a member of the Italian judiciary and the Brussels political class, Buttarelli did not abandon the less fortunate to their fate. In his manifesto, he laments the emergence of a "digital underclass," billions of individuals who subsist on less than two dollars a day, refugees, child laborers, gig economy workers and more, who have weak to no privacy protections and little control over their digital selves. The fate of these people should not be left for market forces to determine or for digital totalitarian powers to dictate. Rather, policymakers in the UN, Europe, U.S. and rest of the free world bear a historic burden, to ensure that in the zeal for development, efficiency and growth, the plight of these individuals for digital selfhood is upheld.

While Buttarelli has left us, his spirit remains. The manifesto, of course, cannot fully capture his towering intellect and racing mind. Rather, it is his students, disciples and protégés, at the Italian Garante, EDPS, Council of the EU, Council of Europe, Lumsa University, and the numerous conferences and workshops he organized and attended, who will carry the torch.

Privacy 2030:
A Vision for Europe

Giovanni Buttarelli wished to publish in 2019 a manifesto on the future of privacy in Europe. The focus would be on what the European Union can bring to the big questions of sustainability, digital technology and human rights, but he also hoped it would inspire discussion beyond Europe. His premature death tragically intervened before it could be finalised. This document does not necessarily reflect the official view of the EDPS but is based on discussions I had with him in his final months. It aims to plot a plausible trajectory of his most passionate convictions.

Christian D'Cunha, Head of Private Office, EDPS

November 2019

I

A NEW MANIFESTO FOR PRIVACY

Data means power

Such power involves the ability to gather information on people, make inferences from that information and, in turn, derive value from it, whether in the form of commercial gain or the ability to shape and coerce human behaviour.

Relatively few wield this power. Data protection aims to constrain it to serve the rights of people to develop their own personalities, have free space to think, keep secrets, speak freely, and form and maintain relationships. It aims to facilitate responsible data processing, including where in the public interest.

Many of us had hoped that digitisation would empower people, like "a bicycle for our minds"

Yet the advance of digitisation has been eroding the room for unmonitored, inviolate freedom. Meanwhile, the share of "value" from digitisation is ever more unevenly spread, a trend that mirrors the growth in inequality over recent decades. A digital underclass has emerged, comprising low-wage workers, the unemployed, children, the sick, migrants and refugees who are required to follow the instructions of machines. These groups are unable or not allowed to understand the logic of the algorithmic decisions that affect them. Rather, many of them are required to train algorithms or repair the damage created by algorithmic decisions. Programming reflects the overwhelmingly white and male bias of its coders. In some parts of the world, powerful external players do not listen to local people, but treat them as mere datasets while mapping and ordering their land as a precursor to its "colonisation."

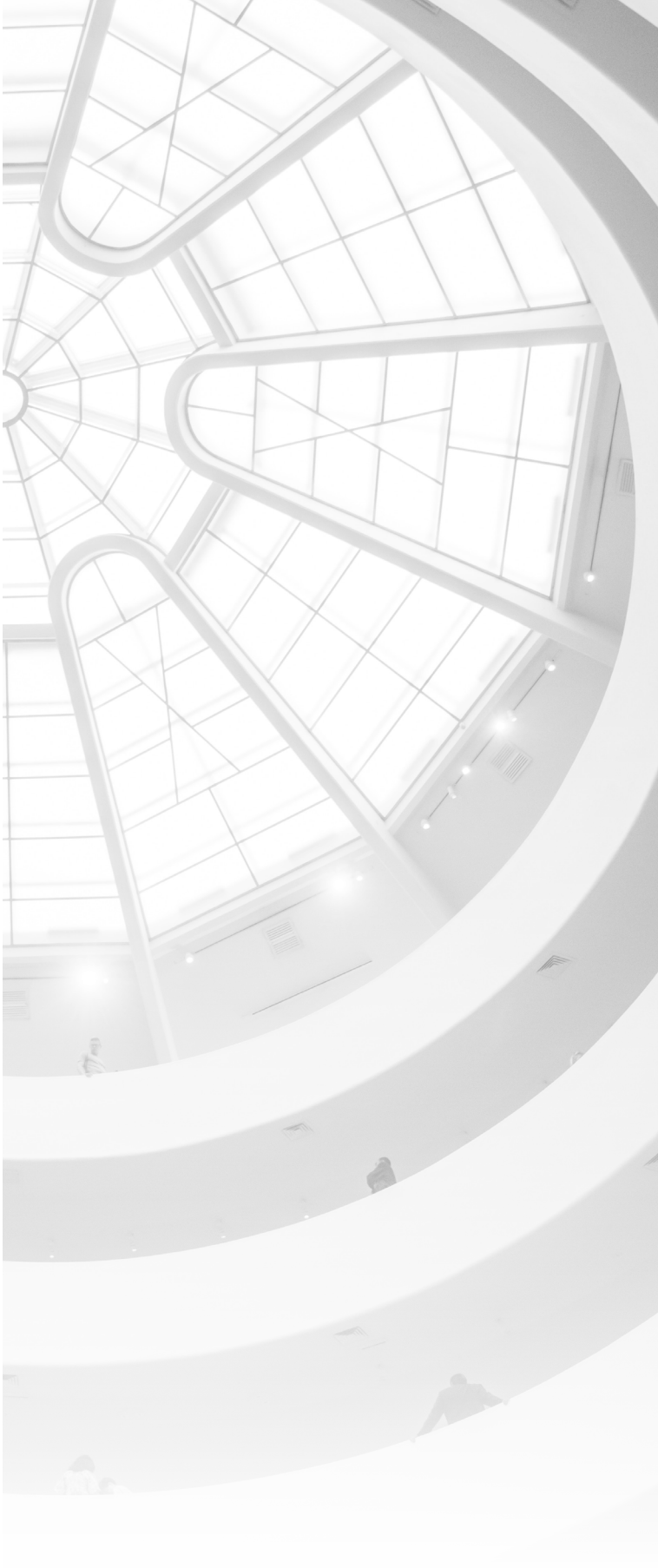
The rush to digitise has had an impact on society and the environment, as well as on treasured norms, such as the rule of law and democracy

Connectivity would appear to be a good thing. But where relationships are mediated by revenue-maximising algorithms and providers are not accountable for the risks inherent in their services, connectivity has contributed to polarisation and the weakening of the social fabric.

In the 20th century, technology, including the internet, was originally designed for military purposes and then later adapted for commercial and private use. In the 21st century, we now see commercial initiatives (smart cities, facial recognition) finding a market among state actors seeking to coerce or repress entire populations and ethnic or socioeconomic groups. These applications are typically justified in the name of "security," "convenience" or "efficiency." There is little regard for the unintended consequences or broader impacts on society and the environment.

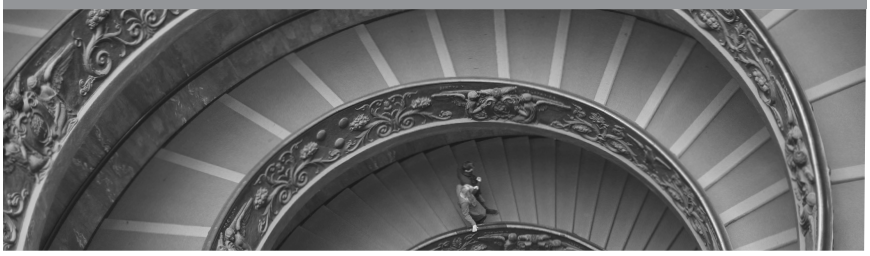
This is not inevitable; it is the result of policy decisions to act or to refrain from acting

The EU's core values are solidarity, democracy and freedom. Its conception of data protection has always been the promotion of responsible technological development for the common good. With the growing realisation of the environmental and climatic emergency facing humanity, it is time to focus data processing on pressing social needs. Europe must be at the forefront of this endeavour, just as it has been with regard to individual rights.



II

A FAIRER ALLOCATION OF THE DIGITAL DIVIDEND



"The future is already here," wrote the cyberpunk novelist William Gibson, "it just isn't evenly distributed."

Digital technology can bring people together and make new things possible. According to the secretary-general of the United Nations, however, "Digital advances have generated enormous wealth in record time, but that wealth has been concentrated around a small number of individuals, companies and countries."

50% of the planet has access to the internet, but the rate of growth has been slowing, and women and poor people are far less likely to be connected

In Europe and across the affluent West, internet connectedness has spread within a broader context that has been described as "an unholy trinity of slowing productivity growth, soaring inequality and huge financial shocks." China and the United States are the global controllers of data. Digital markets are characterised by network effects that tip toward market dominance and "data-opolies." The artificial intelligence industry is also tending toward monopoly, with a concentration of private control over "data collection and experimentation infrastructure."

A gap has grown between people with the means to control technology, their own digital lives and those of others, and people who are objects of the technology and data processing

At the bottom of the food chain has emerged a digital underclass who have weak or no protections and little control over their digital selves. Five out of the 10 richest people in the world are current or former tech CEOs. A child working in a cobalt mine in Congo (cobalt being an essential component in Lithium-ion batteries used in portable devices) would need to work more than 700,000 years nonstop to earn the same amount the richest tech CEO makes in one day.

In recent years, Europe has received 1 million people seeking refuge or a better life, out of a total of 13 million displaced from zones of conflict and climatic disasters. "Irregular" migrants and refugees are subject to exceptional monitoring and control in the EU through existing and planned large-scale IT systems that provide for the processing of biometric data and facial images. Security and migration management are now routinely conflated, effectively treating as potential criminals ordinary, law-abiding families who choose to or are forced to leave their home countries. The EU has funded research into using "smart lie detection" at the EU's external borders.

Workers in the "gig economy" cannot get access to data that rates their performance or determines how jobs are assigned and consequently are unable to obtain a share in the value creation. Workers contracted to moderate appalling content on social media are required to operate in demeaning conditions to be paid a fraction of the salary of those companies' median employees. In dominant ecommerce-driven warehouses, workers have their movements determined by algorithms; recently, a patent was filed for such workers to work within metal cages with cybernetic add-ons. Clerical workers have to work on smart desks monitoring their movements that one described as "an umbilical cord to the computer." AI systems are deployed to replace human caseworkers in mediating between the state and people dependent on welfare support. We are "stumbling zombie-like into a digital welfare dystopia," according to the UN special rapporteur on extreme poverty and human rights.

"Data protection" and "data security" are misappropriated to justify secrecy and unaccountability, contrary to the spirit of the GDPR

A vibrant market for surveillance technologies has enabled states to repress minority groups. In some jurisdictions, the internet functions as "a real time privately run digital intelligence service," for instance, where Uyghurs are forced to install government tracking apps accessible by the police on their smartphones. As the EDPS highlighted, dual-use technologies are now a major concern because of the ability and willingness of authoritarian regimes to harness complex global supply chains and research networks in order to deploy facial recognition, augmented and virtual reality, 5G and quantum computing to repress human rights.

Western and Chinese multinationals have been accused of data colonialism

Particularly in the Global South, tech giants aim to map the territory and establish dependency on their own technological infrastructure, proprietary software and corporate clouds in a process likened to the colonialism of previous centuries. (China, on the other hand, forbids foreign companies from mapping the country.) Access to essential services can therefore be switched on and off at the whim of private companies. Consequently, the Global South, which stands to suffer disproportionately from global warming — itself largely the result of industrialisation in the Global North — stands to become even more susceptible to exploitation.

The rule of law implies legitimacy, fairness and impartiality of a legal process, regardless of outcome

The biggest tech companies are now so enormous that they have had to invent their own sprawling bureaucracy to patrol the impact of their business model on the public sphere. This amounts to an ersatz administration without any democratic accountability. Corporate secrecy and intellectual property rights seem to enjoy stronger protections in practice than individual privacy and personal data. Individual plaintiffs need to spend tens of thousands of euros in legal fees just to get to court and contest violations of the EU General Data Protection Regulation. "We shouldn't have to beg, plead and become technical wizards to exercise our fundamental rights."

Where companies whose goals "do not necessarily encompass the general interest" become more powerful than many sovereign states, democracy and the rule of law are threatened. Data protection authorities, along with other enforcers, face enormous challenges in uncovering opaque business practices to uphold the rights of individuals. These agencies' resources are dwarfed by the legal and lobbying heft of the biggest companies they are meant to regulate. Aggressive corporate resistance to all attempts at regulation and enforcement bely the smooth PR and "dashboards" professing to care about privacy. It becomes a question no longer of budgets and headcount but of whether certain companies are too big to comply. Antitrust, democracies' tool for restraining excessive market power, therefore is becoming again critical. Competition and data protection authorities are realising the need to share information about their investigations and even cooperate in anticipating harmful behaviour and addressing "imbalances of power rather than efficiency and consent."

Privacy policies protect the controller rather than the user of the service; they are rarely consulted and almost never open to negotiation

Although companies offer a veneer of transparency, actually accessing data about yourself seems to become more difficult the larger the company, which contrasts with the apparent ease of finding the data for company insiders. Increasingly, private platforms intermediate the relationship between citizen and state. Data defines individuals and determines how they can be treated. The terms of service therefore become, in effect, the law.

Investment is drawn to technological solutions ostensibly aimed at fixing social problems but, in fact, likely only to exacerbate the digital divide

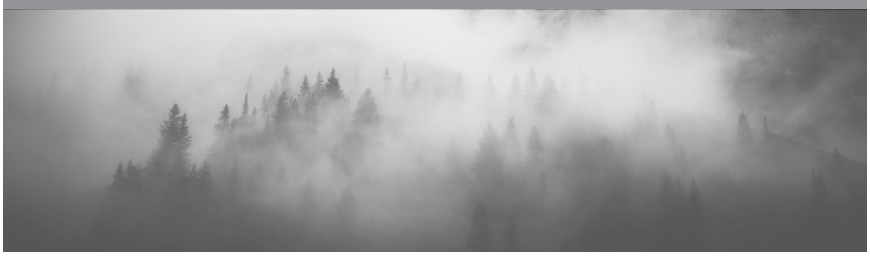
Examples of "techno-solutionism" include initiatives that appear more concerned with insulating the powerful from climate catastrophe than with liberating and empowering. Notions of colonizing Mars, reversing the aging process and uploading one's mind into a supercomputer represent digital reimaginings of "the secession of the rich." They place technology "in an arms race with itself," leaving us "searching for answers with [our] right hand to problems that others in the room have created with their left."

The EU should address not only digital disenfranchisement and lack of access to digital infrastructure and services but also digital inequality

People are social animals, and societies are shaped not just by disadvantage at the bottom, but also by inequality across the spectrum. Societies become dysfunctional when many people see others having more or better. This is the urgent ethical question of our day — not thought experiments, like the "trolley dilemma," rights for robots or whether to allow brain enhancements.

III

A DIGITAL GREEN NEW DEAL: DATA FOR A SUSTAINABLE FUTURE



We are becoming sensitive to the externalities of massive data processing and connectivity; connecting everything has a cost to society and the environment, as well as individuals

We are in a climate emergency, already felt acutely in some parts of the world. Next year, in 2020, we have to "bend the emissions curve" — start to reduce our carbon emissions, and by 2030, we will need to have halved them. Responding to the crisis will touch every aspect of life. Digital technology and privacy regulation must become part of a coherent solution for both combating and adapting to climate change. Alas, at present, they seem like part of the problem. According to the UN Environment Programme, growth in gross domestic product in the last 20 years — the period of rapid globalisation and digitisation — appears to have come at the expense of "natural capital," the world's natural assets of air, soil, water and biodiversity. All regulators will need to converge in their policy goals — for instance, collusion in safeguarding the environment should be viewed more as an ethical necessity than as a technical breach of cartel rules. In a crisis, we need to double down on our values, not compromise on them.

The religion of data maximisation, notwithstanding its questionable compatibility with EU law, now appears unsustainable also from an environmental perspective

Tens of thousands of entities use hundreds of techniques to track people across the web. Tracking and sensors are so pervasive that each of us leaves digital traces, like pheromones, wherever we have been. The enthusiasm for video, AI, facial recognition, wearables and smart devices indicates an inexorable drift to ever more personal data collection and storage — estimated to double energy consumption every four years.

AI's carbon footprint is growing. Industry is investing based on the (flawed) assumption that AI models must be based on mass computation. Training an AI model for natural language processing produces 300,000 kilograms of carbon emissions. One recent technological phenomenon, cryptocurrencies, is estimated so far to have contributed as much CO2 emissions as a million trans-Atlantic flights and consumed more electricity than that generated by all of the world's solar panels combined. Overall, digital technologies are estimated to be responsible for 4% of greenhouse gas emissions, rising to 8% by 2025 and 14% by 2040, while accounting for 8% to 10% of electricity consumption. The opacity and secrecy of the most dominant companies in their respective digital markets prevent scrutiny of their actual environmental impact, so supply chains remain invisible, unlike for other everyday necessities like food and medicines.

Unsustainable development and deployment of digital technology will contribute to its own negative feedback loop

"Smart" devices depend on so-called "rare earths" that are so weakly concentrated in clay that the leftovers end up polluting rivers and hills. Computers have an average lifespan of less than five years (compared with 11 years for a computer in 1985), and are, by design, much more easily replaced than repaired. They are usually not recycled: Toxic e-waste is one of the fastest-growing sources of waste in the EU, often left to be processed in unregulated regions in Asia and Africa. Yet, digital technologies have the potential to monitor and help reduce the consumption of material, enabling innovations, like shared mobility for passenger cars and precision farming.

Tech giants recently supplanted gas and oil multinationals as the most highly valued companies in the world. But the former now collaborate with the latter to locate and extract more fossil fuels and even appear to support climate-change-denying pressure groups. Carbon released into the atmosphere by the accelerating increase in data processing and fossil fuel burning makes climatic events more likely. This will lead to further displacement of peoples and intensification of calls for "technological solutions" of surveillance and border controls, through biometrics and AI systems, thus generating yet more data. Instead, we need to "greenjacket" digital technologies and integrate them into the circular economy.

Vast amounts of data have been collected — however lawfully or ethically — and are now concentrated in the hands of 5 to 10 massive private companies based in the US and China

The question for society is whether this data can be now used for the benefit of individuals and wider society. A "Europe fit for the Digital Age" must be oriented toward the common good and sustainable solutions. Big data, AI and the internet of things should focus on enabling sustainable development, not on an endless quest to decode and recode the human mind.

Independent researchers and academics have great difficulty accessing the data controlled by these enormous companies, a major obstacle to accountability, to understanding the full extent of the harm wrought by their business models. This culture of secrecy and determination to maintain control of the data, is an obstacle to society's need to generalise the potential value of these datasets. There is potential for AI and machine learning to help monitor degradation and pollution, reduce waste and develop new low-carbon materials. These technologies should — a way that can be verified — pursue goals that have a democratic mandate. European champions can be supported to help the EU achieve digital strategic autonomy.

Data minimisation and quality are core principles of EU data protection law. Implementing these principles will help tackle the expanding carbon footprint of digital technology. The GDPR has introduced an obligation to apply "data protection by design" and "by default" — this should complement "durability by design" for new technologies.

Personal data can and should be used to serve the public interest, the general interests of state and society rather than those that benefit distinct groups or individuals

Interference with the right to privacy and personal data can be lawful if it serves "pressing social needs." These objectives should have a clear basis in law, not in the marketing literature of large companies. There is no more pressing social need than combating environmental degradation. The data should not be gathered and used to "legitimis[e] surveillance capitalism — business models that rely on intrusive data collection — and lock society into relying on big tech," nor should trade secrets and intellectual property rights be an obstacle to the public good. The EU should promote existing and future trusted institutions, professional bodies and ethical codes to govern this exercise.

IV

END THE MANIPULATION MACHINE BEFORE THE NEXT GENERATION

By 2030, the children of the first digital natives will be connected

Their parents may already be more skilled than their grandparents in taking control of their own lives in a connected world. "GenZ-ers" use technology to experiment with their identities. Children and young people are nevertheless targeted relentlessly for and by their data. More than half of the most popular content on dominant online video platforms is aimed at children, and it has become a magnet for disturbing images and exploitation. Of course, deplorable behaviour is not to be blamed on digital technology, but digital technology and the power of the major platforms facilitates such social ills at an unprecedented scale. Unlike for copyright-protected material, the targeted dissemination of exploitative content is only halted slowly — citing "free speech" arguments — and after revenue has been generated. Teenagers' preferred social media and "news" platforms are "teeming with conspiracy theories, viral misinformation, extremist memes, all daisy chained together via a network of accounts with incredible algorithmic reach and millions of collective followers many of whom … are very young." These are also the "go-to" network for "active measures" by foreign hostile states aiming to "subvert anything of value in its enemy country — including the justice system." The market for mass internet communications is so concentrated that the big platforms provide an easy target for exploits.

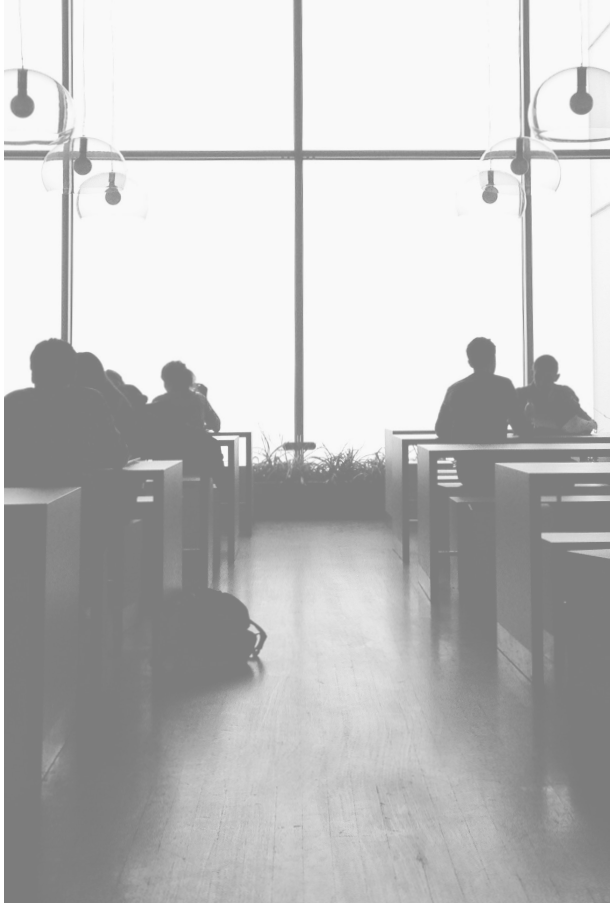
As with the financial system 10 years ago, a vacuum of accountability lies at the heart of the vast adtech ecosystem

People are inescapably profiled into indisputable categories — "people like you" — as earlier generations were assigned a sign of the zodiac. Behavioural advertising is saturated with thousands of intermediaries, most of whom have no direct contact with publishers, advertisers or customers and has become the focus of intense scrutiny.

First impressions of the GDPR indicate big investments in legal compliance but little visible change to data practices. The shared experience is of ubiquitous emails and popups requiring you to accept new terms and conditions. The Cookiebot report on public sector bodies in the EU and the EDPS's on 10 EU institutions' website compliance with data protection rules show how deeply pervasive the model of third-party tracking has become. Even record fines seem to have no effect on business models, but rather seem to be factored into corporate strategies as manageable business risks. True privacy by design will not happen spontaneously without incentives in the market.

Only people with technical expertise can hope to escape the pervasiveness of this "surveillance capitalism" — for example, by using special software to detect tracking of their behaviour. Otherwise, individuals must pay a premium to enjoy privacy.

The vulnerable and unskilled of the next generation will need empowerment and safeguards against this "manipulation machine"



EU lawmakers have strived for 20 years to ensure rules on privacy of communications kept pace with the changes in how people talk to each other. This is not a technical question for the telecommunications sector, for "over-the-top" or any other sectors that will no doubt emerge in the next 10 years as the favoured communications service provider for the children of GenZ. Communications — content and data about content — have to be secure, not least because an authoritarian regime would be as much interested in whom you are talking to as they would be in what is said. However, companies — with less interest than governments in spying on individual behaviour — are fast adopting "optimisation" solutions that encrypt people's raw data while enhancing their ability to profile and manipulate. The EU still has the chance to entrench the right to confidentiality of communications in the ePrivacy Regulation under negotiation, but more action will be necessary to prevent further concentration of control of the infrastructure of manipulation.

The EU should determine the limits of monitoring and monetising people

For a long time, purchasing habits have been considered fair game. Since around 2000, the dominant business model has assumed that web-based services must gather data on interests, relationships, location, gender, race, religion and political views. Unlike traditional broadcasting media, TV and radio, social media facilitates hypertargeting. In the last decade, the proliferation of health and fitness trackers and smart speakers has extended this surveillance into our most intimate physical and domestic spheres. The next frontier is biometric data, DNA and brainwaves — our thoughts. Data is routinely gathered in excess of what is needed to provide the service; standard tropes, like "improving our service" and "enhancing your user experience" serve as decoys for the extraction of monopoly rents.

Notions of "data ownership" and legitimisation of a market for data risks a further commoditisation of the self and atomisation of society. Privacy could become privatised, with only the powerful able to protect their secrets. Business models should serve the social compact, not replace it. The right to human dignity demands limits to the degree to which an individual can be scanned, monitored and monetised — irrespective of any claims to putative "consent."

Digital products need the same rigorous scrutiny for their safety as physical products, like medicines, toys or cars

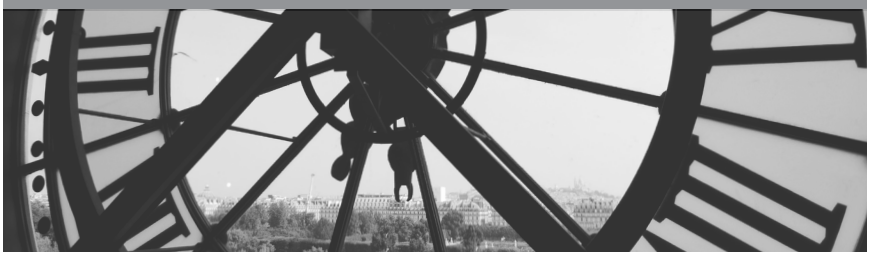
We do not, in the name of "innovation," allow products onto the market where there is risk of harm; no one criticises such precautions as "strangling" innovation. In the words of one critic of the smart-city initiative in Toronto, "When did we as a society say that however we move around in public space — that this is something we want to share and commodify?" The EU is ideally placed to lead this conversation, even at the price of calling a moratorium on certain invasive and dangerous technologies — like facial recognition and killer drones — while the necessary democratic deliberations take their course.

Like for environment, we need a new common understanding of the value and cost of deploying digital technology like AI

Natural capital accounting — a sub-category of environmental accounting — is not yet common but standards for it have been developed in different countries and internationally ("generally accepted accounting principles"). It recognises that all inputs and outputs cannot be reduced to monetary value. It would enable harmful action to be penalised or prohibited and beneficial applications to be incentivised. The incentive structure must be fixed. Damaging behaviour should not be a lucrative business.

V

THE EU CAN DO THIS



By 2030, it is likely that almost all countries in the world will have a data protection framework, due in part to the centrality of data flows in bilateral and regional trade deals

Digital flows now exert a larger impact on economic growth than trade in goods. The EU's considerable global influence as the world's largest trading bloc, second largest economy and pioneering regulator was most recently demonstrated in the agreement with Japan on trade and on adequacy of data protection standards. At the same time, with control over data and communications networks now a geostrategic priority (see for instance the World Trade Organization negotiations on new e-commerce rules), there is an obvious countertrend toward data protectionism (or "localism") rather than data protection.

There will be plenty of laws, and there are already many "GDPR-like" or "GDPR-lite" laws around the world. The GDPR has its competitors as models for personal data regulation. Some commentators doubt whether the GDPR's influence can be maintained, arguing countries may be more attracted to the modernised Convention 108. The "Data Free Flow with Trust" concept promoted at the G20 Summit in June 2019 is not the same as the GDPR rights and accountability framework. Whatever the model, there must, however, be the will and resources to enforce the rules. Individuals and groups must have the means, as well as the legal rights, to raise concerns and be heard. A "splinternet" is not desirable, but it may be inevitable if certain regions of the world cannot safeguard the values of human dignity and democracy.

The EU has enormous leverage for changing the rules of the game — but it is unused because we are torn between our convictions and our aspirations to compete on its rivals' terms

These convictions include minimisation of personal data processing. The aspirations include maximising data collection to pursue the phantom promises of AI. There may be a way of reconciling this contradiction. At a time of environmental crisis and rampant inequality, human capital is undervalued, and natural capital not valued at all in measures of economic growth. Data and technology come at the cost of scarce human and natural resources, and they should not be squandered on dangerous and unsustainable efforts to manipulate the human mind.

Instead, the EU should demand that digitisation address the avowed pressing social and environmental goals that it shares with international bodies, like the United Nations. Its industrial and trade policies should make the deployment of risky technology, such as sensors and autonomous systems, conditional on whether they serve the goal of reducing CO2 emissions and halting the loss of biodiversity. Such applications can only be justified if they benefit everyone, not just a few private actors. Data that has been collected lawfully on people in Europe should be put to work in the general interest of Europe; where there has been systematically unlawful collection and use of personal data, the solution may lie in a form of "amnesty" for those responsible to hand over their optimisation assets.

The EU's research and innovation policies should promote digital innovation where it enables genuine "self-actualisation" and empowerment. This necessitates much more "vertical" dialogue between experts in AI, the environment and civil liberties. Solutions should not prioritise "efficiency" at the cost of societal externalities, or "rebound effects," as has been the case with ride sharing, for example.

The GDPR is a gold standard, but the EU data protection community has to prepare for the next decade

The GDPR alone will not change the structure of concentrated markets or in itself provide market incentives that will disrupt or overhaul the standard business model of tracking and targeting. There is some provision in the GDPR for scalability of obligations. But the GDPR does not systematically address the massive imbalances in power between, on the one hand, major tech companies and governments and, on the other, small competitors, individuals and workers — not to mention vulnerable groups, like children, the socially disadvantaged and migrants. There may be loopholes and deficiencies that will only emerge in the coming years. Many novelties of the GDPR, such as data portability, certifications and privacy by design, have not been implemented or tested.

Already cases have emerged where data protection has been misappropriated to weaken press freedom. Meanwhile, many political parties assume data protection does not apply to them. **Campaigning politicians have no incentive to minimise their own tracking, profiling and targeting of voters and few, if any, to curb the power of platforms that they have come to rely on.** This is a dangerous potential loophole. The EU should forestall such abuses through robust enforcement.

So DPAs need to exercise the full range of their powers

There has been a big relative increase in resources across the board. Data protection authorities should not simply demand additional resources — they need to have courage to exercise their full powers. All supervisory authorities should be confident of their ability to uphold the rights of data subjects in their jurisdiction irrespective of where in the EU a multinational company is established. DPAs have a crucial role in building the case for independent regulation serving interests that go beyond the individual and beyond the national. Every enforcement decision will be contested, with the risk of regulators getting bogged down in court proceedings. Solidarity and consistency among the regulators is therefore essential.

The European Data Protection Board can begin to lead by example on sustainable privacy

The EDPB can achieve carbon neutrality before 2030, ensuring that all their meetings are accessible via video conference and encourage commissioners to participate remotely. **The ethnic profile of the typical European data protection authority, perhaps even more than the Silicon Valley coding community, is overwhelming white.** Agencies in the EU should diversify their own workforce better to reflect the societies they represent by recruiting more people of colour and ensuring gender balance.

The GDPR may not be the final word on the correct balance between proximity to citizens and business and the global dimension

There are regular calls for more convergence in the regulation of digital services. The Bundeskartellamt decision on Facebook is an early demonstration of the possibility that certain behaviour violates more than one set of legal obligations. Article 5 of the GDPR requires data processing to be lawful — that means not only compliant with the the GDPR itself, but also with other applicable laws, including those governing e-commerce, e-government, competition, consumer and environmental protection. **There is no good reason why competition and data protection authorities should not pursue cases jointly where there is a common interest.** If there are legal barriers to such cooperation, national and EU legislators should remove them. Even more crucial, **the EU must guard against the emergence of silos in its digital and environmental policies** where there are separate proposals for major legislative initiatives in the first few months and days of the next European Commission mandate. Digitisation must be integrated with and serve the wider urgent goals of sustainable development.

But efforts at enforcement will never be enough

Personal data generation that does not serve democratically mandated public interests or empower people should be treated like data pollution that has a real-life impact on society and the environment. Incentive structures require reengineering. It should not be profitable, whether in the form of revenue-per-click or leaps in share prices, for privacy to be abused, but all too often it is. The digital market results in externalities whereby value is privatised and costs are socialised. It is not sustainable for high-income countries in Europe and elsewhere to have a per-capita material footprint 60% higher than the upper-middle-income countries and 13 times higher than low-income countries. Therefore, data protection and privacy advocates should be at the heart of national, EU and international debates on **carbon and digital taxation**. The EU's tools that exist or are under development, such as data protection, antitrust and corporate and digital taxation, can be used coherently to redress this injustice. The annual conference of data protection and privacy commissioners, newly titled the **Global Privacy Assembly**, can become the forum for building a global coalition of regulators behind this vision.

We can begin to build a European digital commons

As first mooted by the EDPS in 2016, a digital commons would be free from tracking, manipulation and censorship, a safe place for children and other vulnerable people in line with our values of collective solidarity and individual freedom. It could facilitate the "bonding and bridging" required to rebuild social trust. Building it will require an inclusive debate on what may be commodified and what should remain as commons, where services and resources are not "owned" or enclosed into private "walled gardens" but are open for use by all and subject to "communal obligations" of care.

The myth has taken hold that regulation harms technological development, when, in fact, it simply steers it. The hostility to the ePrivacy Regulation indicates a backlash of the EU's ambition to modernise its privacy norms. There may be questions of productivity and enterprise, but data protection is no brake on the EU's capacity to succeed in AI and other technologies.

As well as investing in sustainable privacy-by-design solutions, the EU can instigate an individual right to **the unconditional and unlimited use of the EU's own digital infrastructure and to strong encryption of communications.** Certain digital utilities, such as searching an online library or forging and joining social and civic networks, have become essential to everyday life and participation in a free society. The EU can require these utilities to be equally and freely accessible to everyone and prohibit discrimination and manipulating of content for the purposes of private revenue maximisation.

We must be optimistic about the future of technology in order to be optimistic about the future of our species and natural environment

The success of the GDPR is not inevitable, but nor is a future balkanised internet or surveillance state. For the EU, the GDPR is still a point of departure not arrival. Computers, data and devices should increase participation, accountability, self-actualisation, "social capital" — and combat the degradation of our environment.

In 1946, Aldous Huxley predicted that "in an age of advanced technology, inefficiency is the sin against the Holy Ghost." Whoever controls the infrastructure for turning data into knowledge will define the meaning of "efficiency," alongside "convenience" and "security." There is a recognised urgent need to curb excessive power in the digital economy. Longer term, the unsustainability of reducing people and the earth to resources for exploitation and trading is becoming clear. We need now to seize the chance to harness the data and technology available for social and environmental good. In this way, Europe can aspire to sovereignty of values as well as of technology.

A 10-Point Plan for Sustainable Privacy

1 Dovetail the EU digital priorities with the Green New Deal to support a programme for green digital transformation, with explicit common objectives of reducing inequality and safeguarding human rights for all, especially displaced persons in an era of climate emergency.

2 Regularise a forum of civil liberties advocates, environmental scientists and the machine learning community to advise on EU funding of research and development into technology that empowers individuals and safeguards the environment.

3 Impose a moratorium on dangerous technologies, like facial recognition and killer drones, and pivot deployment and export of surveillance away from human manipulation and toward European digital champions for sustainable development and the promotion of human rights.

4 Enforce transparency of dominant tech companies so that production processes and data flows are traceable and visible for independent scrutiny.

5 Use enforcement powers to prohibit harmful practices, including profiling and behavioural targeting of children and young people and for political purposes.

6 Begin to build a European digital commons, including through support for open-source tools and interoperability between platforms, a right to one's own identity or identities, unlimited use of digital infrastructure in the EU, encrypted communications, and prohibition of behaviour tracking and censorship by dominant platforms.

7 DPAs to pursue joint cases with competition and other authorities and contribute to design of carbon and digital taxation and reform of antitrust.

8 Design a "data amnesty" programme for powerful tech companies to hand over data for deletion or processing in the public interest in exchange for forgiveness for likely past violations in accumulation and use of the data.

9 EDPB and member authorities to be carbon neutral by 2030 and better reflect gender and ethnic composition of the people whose rights they safeguard.

10 EDPB as the driving force supporting the Global Privacy Assembly in developing a common vision and agenda for sustainable privacy.

Afterword:

THE FUTURE OF PRIVACY AND A VIBRANT DEMOCRACY

Marc Rotenberg

Giovanni Buttarelli left the world a rich legacy of opinions, articles and speeches. His life's work engaged one of the great challenges of our era: how to control the rapid transformation of the human persona into a digital identity. His judgements and recommendations, insights and prodding have helped shape the modern right to privacy and protect human dignity and autonomy.

But it is in the manifesto "Privacy 2030" that he sets out his most ambitious views, reaching beyond the domain of data protection and asking us to consider broader questions of climate changes and sustainability, ethics and human rights. Although captioned a "Vision for Europe," Giovanni invites all us to consider the world that we choose to inhabit and how we are to get from here to there.

As a person in the United States, I have often looked to people such as Giovanni and institutions such as the European Parliament to understand how progress is made. Invariably, I return to one conclusion: If we are to make progress, we must strengthen our democratic institutions, we must have meaningful debate without fear of retribution, we must uplift champions who can speak truth to power, and we must be prepared to hold those who would rule us accountable. The only pathway to "Privacy 2030" is through democracy.

But over the past decade in the United States, we have been asked to embrace "multi-stakeholder dialogues," placed outside of democratic norms, and to support a view of the First Amendment that was never intended by our founders. A law passed by the Congress that once

protected an infant industry now preserves monopolistic giants. It is the internet firms themselves who decide who speaks in Congress, how bills are drafted, which are enacted and which are rejected. The top tech firms now outspend all other companies in Washington. And we now live with the consequences of these decisions.

Democratic institutions are imperfect, easily mocked and often inefficient. But they also reveal the wonder of human decision-making, the ability to resolve conflict without resort to violence, the recognition that each person's view must be given consideration, and the recognition that a democratic system of law can both express the will of the majority and safeguard the rights of the individual.

In the United States, we watched with admiration as the European Parliament debated the provisions of the EU General Data Protection Regulation and then how the institutions of the European Union worked together to produce the final outcome. There was conflict and disagreement. There was the "air-lifting" of business lobbyists to Brussels, and there were the famous 4,000 amendments. But there was little doubt that there was a common purpose and a fundamental respect for the institutions that made possible such an achievement. The young democracy is also a vibrant democracy. David Bernet's film "Democracy" about the enactment of the GDPR captured this spirit. I hope someday a similar film will be made about a similar achievement in the United States.

Giovanni understood well the importance of democratic norms and the risks of allowing the siren call of new technology to steer us to hazards from which we could not return. And in setting out his manifesto, he anticipated, I am sure, that there would be disagreement and criticism because that is how, in fact, progress is made.

The world is already confronting two very different futures, shaped by the technologies and policies for artificial intelligence.

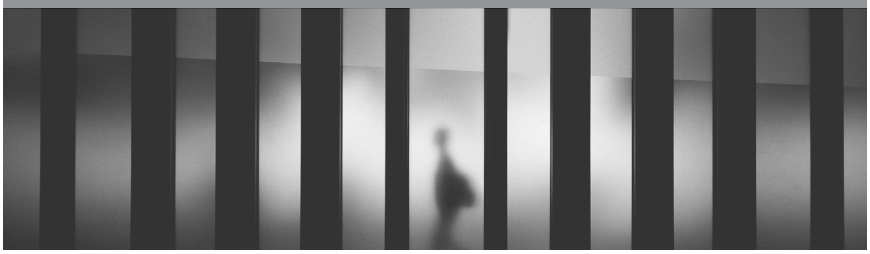
Giovanni also recognized the need for an "urgent" debate, expressing both frustration with the thought experiments of academics and a growing awareness of the pace of change. The world is already confronting two very different futures, shaped by the technologies and policies for artificial intelligence. One may preserve democratic institutions, the rule of law and safeguards for individuals. The other will almost certainly combine the power of automation and logic of efficiency with a growing scarcity of resources that will leave us all as little more than data points, subject to systems we do not understand and cannot control. Such moments in history require a call to action.

And so Giovanni leaves us with both a vision and a reminder. The vision is his manifesto, informed by his many years as a leading authority with recommendations that we should move forward. But there is also a reminder that whatever vision of the future we choose to pursue, there is no progress without democracy and the rule of law.

Afterword:

THE FUTURE IS ALREADY DISTRIBUTED — IT'S NOT EVENLY JUST

Malavika Jayaram



If I'm taking an enormous liberty by paraphrasing the great William Gibson, it's because I know Giovanni would have approved. Not because he was no stranger to wordplay, and not because he often drew on literature and pop culture to communicate complex messages. He would have approved because my remixed message is something he deeply believed in.

Eight words into his manifesto, he's talking about power. Three paragraphs in, he's referencing inequality, the digital underclass, algorithmic bias and colonization. These are not the words of a man who saw privacy as a European project or through the lens of development alone. Calling out the uneven allocation of the digital dividend and the disproportionate impact of privacy harms on the poor and marginalized, he is highlighting parallels with the climate crisis. Just as those who contributed the least to environmental damage will suffer the most, those who didn't design technologies that are ubiquitous and insatiable stand to suffer more than those who did.

Reiterating that large parts of the world are passive recipients, not active participants with agency and autonomy, he is warning that this cleavage will hurt everyone. By elevating issues of access, inequality and disenfranchisement above trolley problems and robot rights, he is focusing on the structural and systemic factors that make societies dysfunctional and pose the greatest ethical dilemma. I read his manifesto as calling on Europe to lead by example, not privilege. He sees that it's a fool's game to treat the data ecosystem as anything other than a collective, global time bomb, even if the ticking is louder in some places than others.

My own interest in the field was catalyzed by a return from Europe to Asia, 15 years ago. My experience in private practice led me to think data protection was for legal nerds obsessed with compliance. It seemed a relatively straightforward formulaic exercise in the context of mergers and acquisitions, until I ran headlong into the complete lack of protection in my new home. The lived reality of a developing economy gathering all the data with none of the safeguards made me experience the idea of privacy in a very visceral way.

Giovanni enjoyed my tales of the privacy invasions I experienced, everything from salacious interest in my personal life to the challenges of critiquing biometric ID systems against a modernizing, progress narrative. He particularly enjoyed my annoyance at generalizations about Asians and privacy. Confronted by people telling me I'd "been away too long," "become too European" and "forgotten that Indian culture is lived entirely at the collective, not individual, level," I would ask if their parents knew they were gay/ate beef outside the family home/smoked/had a partner from a different religion. Using a culture of (selective) secrecy to begin a discussion about privacy and contextual integrity, rather than throwing chapter and verse about human rights, was something that immediately resonated for Giovanni.

He was a champion of efforts to unpack social, cultural, and legal norms and of attempts to locate the local against the regional and the global. We collaborated during the 39th ICDPPC conference in Hong Kong (where I was based then), with EDPS, the UNSRP and Digital Asia Hub co-hosting a side event on "Thinking local, acting global: exploring common values that underpin privacy." He also supported a two-day conference that we put together, focused on "Asian Perspectives for Privacy as a Global Human Right." He had started to use the language of ethics to discuss many of the rights at stake — in this, as with many other things, he proved an early adopter. By the time he organized the 40th ICDPPC around the theme of ethics, he came up against the emerging backlash against a discourse that was being challenged as soft, ineffective and lacking enforcement.

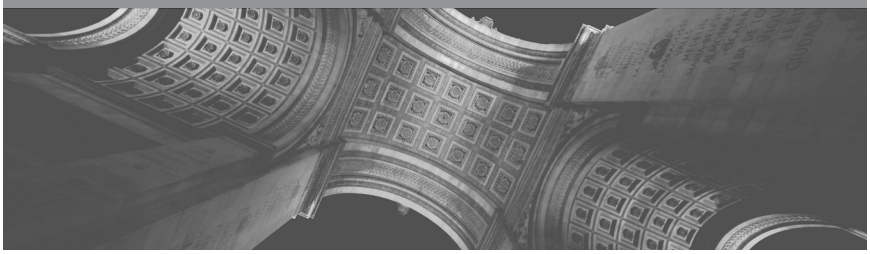
Returning to the language and terrain that he was most at ease in — that of privacy, society, freedoms and values — he left behind an urgent call to arms.

He seemed to intuit that, for all its flaws, ethics afforded a relatively accessible vocabulary to bring different stakeholders to the table. His initial interest preceded the more deliberate and vigorous pushback against "ethics washing" that we have since seen and seemed founded in a desire to work across the aisle and be pragmatic. His manifesto, interestingly enough, does not use the word even once. Returning to the language and terrain that he was most at ease in — that of privacy, society, freedoms and values — he left behind an urgent call to arms. Urging critical engagement with questions of citizenship, participation, identity and autonomy, even if he didn't describe them as such. Ultimately, it is this interest in humanity, warts and all, that I will remember, along with his optimism, that a malign technologically mediated future is not inevitable.

Afterword:

A MISSION GREATER THAN COMPLIANCE

Jules Polonetsky



I am humbled by Giovanni's request to comment on his manifesto, as I was so often humbled by his gracious courtesies to me and the Future of Privacy Forum during his many years in public office. We often disagreed, as I bring more optimism to the debate about the future of tech and data and less faith that government has all the solutions. But we both agreed that unfettered, the excesses of data collection would lead to an Orwellian society and that those who saw the risks needed to press for limits, controls and oversight to ensure the benefits of technological advances would contribute to human welfare. It's with great humility that I offer my comments on his manifesto and my regret that he is no longer on the playing field to continue to debate and to refine his views. Of some solace is that his vision is carried forward by Christian D'Cunha in this effort and by the many of his colleagues in the European Data Protection Supervisor community who carry on the strategies he defined.

In "Privacy 2030," Giovanni sets out a vision for Europe, but his vision might be understood as a vision for democratic countries. Every free society on the planet is struggling with the same digital issues Giovanni engages. The headlines everywhere are filled with concerns about the excesses of surveillance, power of tech platforms, impact of automation and exacerbation of inequality in the data-driven economy. Europe has led the way with regulatory measures intended to counter these concerns, but the rest of the world is rapidly joining in. Even in the

U.S., where "permissionless innovation" has been a driving philosophy, states are moving quickly to regulate, and the federal government will not be far behind. Indeed, regulating tech may be one of the only issues that bring Democrats and Republicans together.

And if there is to be a united front against those countries seeking to weaponize data and undermine democracy, it will require a global alliance of free societies who can work in international coalitions to counter these threats.

Furthermore, it's reasonable to examine whether a European-only regulatory path would be the most effective in resetting the moral balance of power between data and the citizen in a world where economies are linked, academic research is collaborative and people are mobile. An app that operates in an odious manner may avoid the reach of the EU General Data Protection Regulation by avoiding targeting or monitoring Europeans, but the open borders of the internet may make it accessible and popular. The knowledge gained by unethical research in one society is published and the learning available to all. And if there is to be a united front against those countries seeking to weaponize data and undermine democracy, it will require a global alliance of free societies who can work in international coalitions to counter these threats. Given the views of current leadership in the U.S., it does fall to Europe to lead, but I urge a vision of global leadership and cooperation to be effective. Giovanni takes note of a number of pathways, and there are many more, including standards bodies and the Organisation for Economic Co-operation and Development.

Giovanni calls on the data protection authorities to exercise the full range of their powers. In particular, he notes the need to provide local DPAs with the confidence they need to uphold rights of the data subject in their local jurisdiction, regardless of company establishments. One path to address this challenge while respecting the GDPR's one-stop-shop imperative is to foster joint investigations and joint enforcements by DPAs. The success of state Attorneys general in the U.S. in taking on the likes of big tobacco makes clear the resources and power wielded when groups of attorneys general band together to manage investigations and cooperate in litigation. This is also a situation preferable for companies because they are able to organize one standard and one settlement rather than deal with multiple fronts. Individuals gain, as well, since the collective group of enforcers is often able to gain penalties and corrective action that is broader than any single enforcer might have achieved.

"Privacy 2030" touches on a wider sweep of ideas than can be addressed in a short essay, but they all are ideas inspired by the opening theme of the paper, the argument that "data means power." Giovanni's greatest contribution in this paper and perhaps in his tenure at the EDPS is his insistence that we see the impact of data on social welfare, for better and for worse. His call for action should motivate all us working in this sector to recognize that our mission is far more than compliance and data protection. As our social and commercial lives are increasingly mediated by technology and data, we must meet Giovanni's challenge by using all the tools at our disposal to ensure technology and data are forces for good in society.

Afterword:

"A CAGE WENT IN SEARCH OF A BIRD"

Maria Farrell

Franz Kafka certainly knew how to write a story. The eight-word aphorism he jotted down in a notebook a century ago reveals so much about our world today. Surveillance goes in search of subjects. Use-cases go in search of profit. Walled gardens go in search of tame customers. Data-extractive monopolies go in search of whole countries, of democracy itself, to envelop and reshape, to cage and control. The cage of surveillance technology stalks the world, looking for birds to trap and monetise. And it cannot stop by itself. The surveillance cage is the original autonomous vehicle, driven by algorithms it doesn't even control. So, when we describe our data-driven world as "Kafka-esque," we are speaking a deeper truth than we even know.

Giovanni knew this. He knew that data is power and the radical concentration of power in a tiny number of companies is not a technocratic concern for specialists but an existential issue for our species. Giovanni's manifesto, "Privacy 2030: A Vision for Europe," goes far beyond data protection. It connects the dots to show how data maximisation exploits power asymmetries to drive global inequality. It spells out how relentless data-processing actually drives climate change. Giovanni's manifesto calls for us to connect the dots in how we respond, to start from the understanding that sociopathic data-extraction and mindless computation are the acts of a machine that needs to be radically reprogrammed.

Running through it all is the insistence that we focus not on big tech's shiny promises to remake the social contract states seem so keen to slither out of, but on the child refugee whose iris-scan cages her in a camp for life. The manifesto insists we look away from flashy productivity PowerPoints and focus on the low-wage workers trapped in bullying drudgery by revenue-maximising algorithms. The manifesto's underlying ethics insist on the dignity of people, the idea that we have inherent worth, that we live for ourselves and for those we love, and to do good, and not as data sources to be monitored, monetised and manipulated.

But the cage isn't the technology; the cage is our flawed and narrow assumptions about what technology can do.

You don't have to be a Catholic to insist that we ditch cute, reductionist mind-games, like the "trolley problem" to decide who wins and who loses, and insist that technology ethics are instead grounded in respect for people. And you shouldn't have to sound radical to insist that tech business models must serve and be accountable to us, not the other way around.

The manifesto and its "10-Point Plan for Sustainable Privacy" show there is another digital path forward. Not the oppressive brittleness of China's state sovereignty model, and not the colonialist extraction of Silicon Valley. There is a European Union version of the internet that starts with the society we as citizens want to live in and then figures out how to get there. It recognises that just as we don't live our lives to serve corporate interests, nor must we sacrifice our private and public spaces to serve the state. Because in any future, we actively want to live in, autonomy is for humans, not machines.

The European vision of our digital future will take the work of many of our lifetimes to achieve. That eight-word story doesn't have an ending we can yet see. The surveillance cage cannot help but try to trap birds. That's its programming. That's just what it does. But the cage isn't the technology; the cage is our flawed and narrow assumptions about what technology can do.

The manifesto says we must be optimistic about the future of technology so we can be optimistic about the future of our world. It's right. Right now, technology itself is in the cage. There is so much more technology can do — banish inequality, repair our environment and support us all in living our best lives — if we cut it loose from the business models that entrap us all.

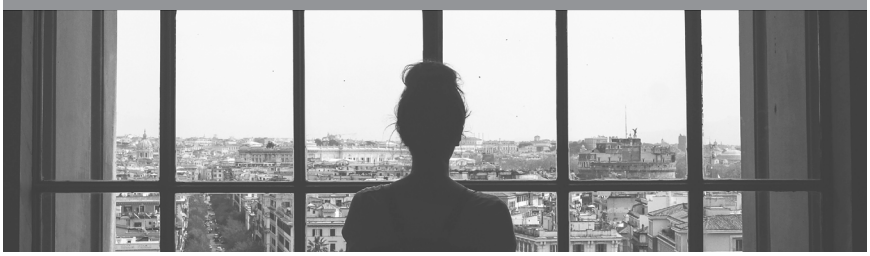
When indignant interviewers asked Giovanni if Europe was imposing its views about privacy on the rest of the world, he would reply courteously that Europe was just setting an example. (Countries figuring out how to secure an adequacy finding may disagree!) But he was right. Just the fact that a major trading block insists in both word and deed that there is another way, that we actually have a choice of digital futures, is almost enough.

Almost.

Afterword:

PRIVACY 2030: TO GIVE HUMANS A CHANCE

Rocco Panetta



To fully understand the thought of Giovanni Buttarelli, it is from Rome that we must leave and start our journey for discovering the milestones of his powerful word, and like in a virtuous circle, it is in Rome that we must return.

All the thought and action that characterized the extraordinary professional experience and legacy of such a modern-day giant that was Giovanni Buttarelli moves from two pillars: first, from the study and heritage of another immense and fruitful thinker of the 20th century, what was the jurist Stefano Rodotà, one of the fathers of the European privacy and data protection laws; and second from the unrepeatable and exceptional gym represented by the years in which together Rodotà and Buttarelli built and launched the Italian data protection authority, the Garante per la protezione dei dati personali, in Italy, an institution's growth on the fertile ground in between two of the most valued and strong bills of rights: the Constitution of the Republic of Italy of 1948 and the Chart of Fundamental Rights of the European Union of 2000.

The manifesto is a natural product of this ground, a treasure chest containing a number of visionary ideas, some of them representing the state of art of the relationship between our society and the issue of the personal data processing, especially as affected by the technology development, while others focusing on the dangers of a deregulated digital world, in the hands of players, sometimes acting in the absence of a strong and shared line of contrast on the part of national and supranational institutions.

Where to start from? By the law and by the rules of the European Union, of course. This is a European story spreading all around the world.

The human experience must not and, above all, cannot be reduced to a (digital) commodity.

The strength of this posthumous work lies in its slipping in the wounds that most threaten contemporary society: digital inequality and discrimination capable of exponentially increasing the information asymmetry between rich and poor, increasingly marked disparities between the north and south of the world, dramatic environmental crisis, also caused by an uncontrolled production of high-tech devices and an unprecedented energy consumption that these devices require, the will to shape the young and the very young, to the point of affecting the cognitive and relational processes to which the XXI century had accustomed us to it.

The accent is further placed on the effects that uncontrolled profiling through algorithms-generates money produce on reality as a consequence of a sort of digital colonization.

The observations relating to the upcoming ePrivacy Regulation in the European Union are paramount. This legislation, complementary to the EU General Data Protection Regulation, is perceived by Buttarelli as another and necessary bastion of maintaining effectively confidential communications — a fundamental right in most countries around the world which is under an increasing and unprecedented pression.

The refusal for a vision of data ownership is clearly perceptible in the Buttarelli's vision. The monetization of people must be stemmed and limited by EU legislation and restored the value of what is secret as a condition of freedom, not only for the rich and powerful Western white people. The human experience must not and, above all, cannot be reduced to a (digital) commodity.

The European regulators, DPAs in the first place, must be courageous, to the point of questioning and rethinking the structures, the workforce and the tools through which to direct and protect the choices linked to the world data market.

The question that arises is whether the current EU effort is sufficient to stem the way in which the big tech, especially those coming from the two powerful economic systems, are shaping the world.

It is worth noting that in this sea of technologies, digital tycoons and deregulated algorithms, we are all involved, without exception. Unlike the past, where changes of direction had a strong national matrix, the political boundary today can and must be crossed, just as profiled clusters qualify network users globally, regardless of where the multinational is located or from the place where the user connects.

In the vivid and lucid Buttarelli's vision, all contemporary problems are linked together and led to the threatening of freedom and democracy society: environmental issues, climate change, migration flows, poverty and inequality, sovereignism and white supremacism are exacerbate by a technological fever and a data-processing bulimia.

Some positions echo more soundly than others, especially because they are expressed by a man who, until a few months ago, was the head of a European institution, the EDPS, and that in the recent past has served with dedication a national supervisory authority and boasted a commendable juridical cursus honorum in his home country and abroad.

The manifesto revolves around the concept of illusion-disillusion vis-à-vis the process of digitization/technological development (e.g., utopias conceiving internet as an unexplored land of the free where to rebuild a new and unbiased democratic society). From the equivalence data equals power, to the polarization of decision making and commodification of digital selves, the hopes for a new age of democracy have been immolated on the altar of a rapid-growing and ubiquitous technological progress.

One of the solutions may consist in a call for a "new humanism," as agreed and proposed at different levels and occasions by many of us, where the human being is put in the center of the political and lawmaking discourse.

The manifesto underlines the non-necessary nature of this state of things, which is instead the result of actions and often omissions of economic players, legislators, media and policymakers. As it is commonly known, an age of deregulation brought the mentioned fast-paced growth jointly with a number of relevant collateral effects (negative externalities). One of the solutions may consist in a call for a "new humanism," as agreed and proposed at different levels and occasions by many of us, where the human being is put in the center of the political and lawmaking discourse. However, we are conscious that a similar radical approach is not free from different albeit comparable negative effects, including recession, stop of investments, unemployment, economic inequality, etcetera.

This new age of capitalism is moving in a direction where the production of goods and services will be more and more centralized in the hands of fewer companies, able to cover most of the needs of the population using data-fueled technology. Keeping on the foreground all the important considerations concerning the use of personal data to enrich business models, goods and services, the views conceiving the technological development as an asset of the collectivity and that, for this reason, believe that revenues shall be shared in a more equal manner should not be considered naïve. If from an ethical standpoint is unconceivable, it is also a matter for economic analysis of the law experts, who should be able to find out a balancing point between incentives to the production and equal redistribution of the generated wealth.

From a data protection perspective, interesting and proactive principles as the privacy by design and that of accountability will never have any effectiveness until appropriate and proportioned incentives will be deployed. At the same time, the noncompliance should be less convenient not only due to the presence of important pecuniary sanctions (like those provided for by the GDPR by reaching a magnitude up to the 4% of the global turnover of the data controller/processor), but also thanks to measures more scary for players-data-eaters, like the block, stop and freeze of data processing.

Considering that competition on data protection added value is currently unrealistic (independent, privacy-oriented projects are eons of light years far from being able to provide services comparable to those offered by the incumbents), we shall expect a different division of the markets, not driven by competition rules and authorities but ruled by ethical principle, like those engraved in the privacy and data protection current laws, like the GDPR.

The GDPR is only a drop in the ocean. EU has the political, legal and policymaking firepower to tackle the issue(s) but should grow and become a clear strong and autonomous third player between the different economic and political blocks. In addition, it is of the utmost relevance that member states align themselves regarding their internal lawmaking choices. Slight differences and nuances are welcome, but the "new humanism" with the human being as the center of any political discourse regarding technology and use of data cannot wait longer and a first concrete step could be to strongly say that the direct monetization of personal data, by means of paying individuals for the processing of their data is not an (ethical) option.

The use of new technologies to exacerbate the blatant violations of human rights should be always kept in mind to have a tragic window on the risks of dystopian and authoritarian futures while, on the other hand, it is not a novelty that political regimes make use of any available technological means to improve their ability of controlling and regulating the lives of their people.

Algorithms and artificial intelligence shall undergo an "ethical due process" irrespective if used in the private or public sector. The European institutions already submit to this exercise, for example, any research project proposal that requires public funding: Thanks to the action of the ERCEA, the European Research Council Executive Agency — of which I have the honor of being one of the ethical experts participating in the related assessment panels — the ethical value of any research proposal become the pivotal element for the issuance of the grant. New technologies shall be deployed on the market only after ethical tests aimed to assess the level of risk for rights and freedoms of individuals.

Similarly, given that new and intelligent technologies imply an inner risk for harming individuals, segregating social classes, discriminating vulnerable people and minorities, favoring unethical behaviors, etcetera, the precautionary principle shall be adopted — interrupting the development until the uncertainty remains (the precautionary principle works in a similar fashion in the field of environmental law).

We have to accept the fact that we cannot have both new services, unprecedented features, transhuman abilities and protection of fundamental freedoms. Policymakers need to set the lever according to the project of society they have in mind: Giovanni had a clear picture of a society more human-centric. Will we be able to do the same and collect his witness?

Let's give humans a chance.

The author wishes to thank Federico Sartore and Marta Fraioli for their useful inputs during the brainstorming and debate on the Giovanni Buttarelli manifesto held at Panetta & Associati before drafting the present notes.

Afterword:

MANY FACETS OF THE SAME DIAMOND

Shoshana Zuboff

The young activist Greta Thunberg put the case succinctly: "Our house is on fire." Global warming is to the planet what surveillance capitalism is to society. If the planet is our house, then society is our home, and it too is on fire, overrun by an audacious and self-authorizing new power. Instead of rising sea levels, it produces rising levels of illegitimate unilateral digitalization ripped from our most private experience without our knowledge. This new instrumentarian power deprives us not only of the right to consent, but also of the right to combat, building a world of no exit in which ignorance is our only alternative to resigned helplessness, rebellion or madness. Giovanni Buttarelli understood this with every fiber of his being.

We have been drawn into the dangerous illusion that privacy is private — a trivial tradeoff for useful commercial services, a personal calculation whose consequences are strictly personal. We failed to reckon with the fact that privacy is a collective action problem, inseparable from the same history that birthed the psychological individual, the discovery of individual sovereignty, inalienable human rights and the very idea of democracy. These elemental themes are joined at birth, many facets of the same diamond. Societies that cherish privacy also cherish freedom and the dignity of the individual. Those that reject privacy, enshrine certainty as the dominant principle of social order. Certainty can only be achieved with tyranny, whether it is the tyranny of the autocrat or of the computational machine.

Giovanni Buttarelli understood these deep lines of Western history. He devoted himself tirelessly to warning Europe and the world of what is at stake. He burned with outrage, but he trained on hope and hard work, leading lawmakers and citizens in the long art of constructing the regulatory vision that would assert an alternative digital future compatible with the aspirations of democratic peoples.

The surveillance capitalists do not content themselves with owning and operating the internet. They want more, and they do not hide their ambitions. Facebook wants to internalize the financial system and the courts. Google wants bodies, homes, cars, cities and regions. Amazon wants to own everyday life, where it lives everywhere and knows everything. Microsoft wants the indexibility of all people, places, objects. Each of these is enmeshed in complex ecosystems and partners: data supply interfaces, market makers and market players. All these derive revenues from buying and selling future human behavior.

Lawmakers have been silent for too long or they have allowed the details of rule making to obscure the emergency that cries out for democratic control over surveillance capitalism. Lawmakers have been easily intimidated by carefully honed propaganda: "Law will stifle innovation." "Market players must be free." "People like free services and are happy to pay with their privacy." "Surveillance capitalism and its assault on individual freedom and democracy is simply the inevitable consequence of digital technologies in a new modernity."

Each of these false arguments has protected the ungoverned growth of the last two decades. They have successfully obscured the fact that this growth originates in the secret theft of human experience as free raw material for datafication, computational production and sales. These foundational acts of theft are wholly or partially responsible for the vast market capitalizations of the four leading surveillance capitalist firms: Google, Facebook, Amazon, Microsoft. These empires are built on the quicksand of toxic assets.

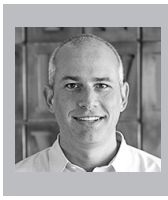
The digital century was to have been democracy's Golden Age. Instead, we now enter the third decade of the 21st century marked by extreme new concentrations of knowledge and power that threaten to remake human nature and society as they unmake democracy. It is time for the sleeping giant of democracy to awaken.

Surveillance capitalists are rich and powerful, but they are not invulnerable. They have an Achilles heel.

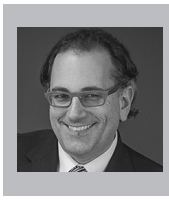
A beloved warrior for democracy has fallen, and the call now is for a thousand more to take his place. Surveillance capitalists are rich and powerful, but they are not invulnerable. They have an Achilles heel. They fear law. They fear lawmakers who do not fear them. They fear citizens who demand a new road to the future.

Come! Let us fight this fire together!

Contributors



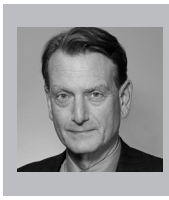
Omer Tene is vice president and chief knowledge officer at the International Association of Privacy Professionals.



Jules Polonetsky serves as CEO of the Future of Privacy Forum.

Christian D'Cunha is the head of the Private Office of the European Data Protection Supervisor.

Maria Farrell is an Irish writer and speaker, based in London.



Marc Rotenberg is president of the Electronic Privacy Information Center and author of "Privacy in the Modern Age: The Search for Solutions."

Rocco Panetta is founding and managing partner of Panetta & Associati, as well as the IAPP Country Leader for Italy.

Malavika Jayaram is the executive director of Digital Asia Hub and a faculty associate at the Berkman Klein Center for Internet and Society at Harvard University.

Shoshana Zuboff is the author of "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power" and Professor Emerita, Harvard Business School.

Featured photographs by:

(pg. 3) Yohann Libot
(pg. 6) José Martín Ramírez C
(pg. 7) Drew Patrick Miller
(pg. 8) Yoosun Won
(pg. 9) Alessio Maffeis
(pg. 10) Drew Patrick Miller
(pg. 11) Markus Spiske
(pg. 12) Kyaw Tun
(pg. 13) Fabian Irsara
(pg. 14) Ryan Searle
(pg. 15) Yiran Ding
(pg. 16) Henry & Co.
(pg. 17) Jordan Whitt
(pg. 18) Adam Przewoski
(pg. 19) Timon Studler
(pg. 20) Evan Provan
(pg. 21) Murray Campbell
(pg. 22) Markus Spiske
(pg. 23) Zane Lee
(pg. 24) Matthew Henry
(pg. 25) Andrew Butler
(pg. 26) Daniel von Appen
(pg. 27) Andy Beales
(pg. 29) Charles Forerunner
(pg. 31) David Werbrouck
(pg. 33) Noah Rosenfield
(pg. 35) Jimmy Chang
(pg. 37) Cristina Gottardi
(pg. 41) Philippe Mignot

Published by IAPP, November 2019.