Perspectives on Privacy and Effective Data Use in the Global Digital Economy and Society

Centre for Information Policy Leadership (CIPL)

20th Anniversary Essay Compilation

Perspectives on Privacy and Effective Data Use in the Global Digital Economy and Society

The Centre for Information Policy Leadership, a global privacy and security think tank founded in 2001 by leading companies and Hunton Andrews Kurth LLP, is celebrating 20 years of working with industry leaders, regulatory authorities and policy makers to develop global solutions and best practices for privacy and responsible data use.

To mark this occasion, CIPL has compiled a volume of short "thought pieces" under the general title of "Perspectives on Privacy and Effective Data Use in the Global Digital Economy and Society". This compilation features contributions from academics, technologists, former regulators and other thought leaders in privacy. Prior to the release of the full compendium, CIPL has posted the contributions individually on a weekly basis on CIPL's blog, "A Very CIPL Solution".

About CIPL

The Centre for Information Policy Leadership is a global think tank which encourages responsible information governance. Through collaboration with industry leaders, civil society, consumer organizations and government representatives, it explores innovative and pragmatic approaches to global policy issues, seeking to build privacy and data protection in practice while balancing economic and societal needs and interests.

During the past two decades, CIPL has evolved into a global organization at the forefront of cutting-edge policy issues. Perhaps most notably, CIPL is known for its extensive work on privacy accountability and its advocacy for the implementation of accountability frameworks and measures by organizations around the world.

Building on this prior work, CIPL has most recently been working with experts in the EU and multinational companies who are leaders in AI, to collect best practices and emerging trends in AI accountability. CIPL's objective in this work is to inform the current EU discussions on the development of rules to regulate AI. More details about the Centre can be found at www.informationpolicycentre.com.

Foreword

On the occasion of the 20th anniversary of the Centre for Information Policy Leadership (CIPL), I am pleased to present this compendium of insights from leading academics, former regulators, privacy experts, and other thought leaders with whom I have had the pleasure and privilege to work and collaborate over the years. A huge thank you to all of our contributors! These 23 short essays cover a wide range of complex issues in today's digital economy and society, such as facilitating organizational accountability, addressing regulatory discord among privacy regimes, clarifying concepts of data protection, fostering trust in the digital economy, managing cross-border data flows, embracing information "climate change", reconciling privacy and innovation, supporting women and online privacy, exploring privacy in the context of democratic societies, championing data ethics, studying neurotech and privacy of the mind, forecasting US privacy, examining outcome-based regulation, analyzing globally interoperable privacy laws, assessing scientific research and health data governance in the age of COVID 19, the intersection of competition and privacy, and so much more.

This seems like a wide range of topics, but they reflect only a small slice of the issues CIPL has been actively working on since our founding 20 years ago. While the scope of our work has broadened from data privacy to, more generally, data policy fit for the 21st century, our mission has stayed the same: to enable effective data use and innovation while also ensuring robust privacy protections. This is at the heart of all our work, whether it be in the context of AI, data sharing, organizational accountability, corporate digital governance, the metaverse, or neuro technologies. As a global data privacy and data policy think-and-do tank, we have worked tirelessly with business leaders, academics, regulatory authorities, and policy makers around the world to develop global solutions and best practices for privacy and responsible data use, always trying to engage constructively and raise the standard of our collective expectations of each other—businesses and regulators alike.

The essays included in this compendium demonstrate the sophistication and maturity of our collective thinking and our grasp of the challenges and opportunities presented by the digital transformation and the 4th (and 5th) industrial revolutions. We have all come a long way, and there has never been a better time to work on the intersection of law, policy and technology in privacy and the digital space generally. I am excited about the next chapters of our collective journey, and I can't wait to continue our work together with all of you—CIPL members, our policymaker and regulator colleagues and friends—to help shape the next generation of data laws, policies and best practices. May we collectively succeed in facing the many challenges and realizing the many opportunities the digital age still has in store for us!

Bojana Bellamy
President, CIPL

Table of Contents

ACCOUNTABILITY AND THE HUMAN HEART

Project Bijou in Guernsey

By Chris Docksey, Hon. Director General, European Data Protection Supervisor | Member, Guernsey Data Protection Authority | Advisory Board Member, European Centre on Privacy and Cybersecurity (ECPC) at Maastricht University

For many years regulators, legislators and powerful influencers such as CIPL and the IAF have been working on how to encourage accountability. At the 2019 ICDPPC, in my Keynote on Accountability, I argued that top management and in-house privacy professionals should be addressed first.

Whilst staff have a key role, they tend to be addressed under the rubrics of "training and education" (*per* the second "common element of accountability" identified by the ***Galway Project*** in 2009). Along the same lines, global regulators resolved at the 2019 Conference to address the role of human error in personal data breaches and committed themselves to "building workplace cultures where privacy and personal data security are organisational priorities, including through the periodic implementation of training, education and awareness programs for employees."

The Guernsey ODPA has launched a wholly new approach aimed at promoting cultural shift by *individuals themselves*. ***Project Bijou*** addresses individuals across the whole of Guernsey, whatever their function or status, as persons who are themselves affected by good or bad data processing. It is a social initiative that encourages its participants to positively influence outcomes in how personal data are treated.

The method is quite unique - people telling stories. Participants are encouraged to talk about their personal experiences inside their organisations, about the benefits of getting data protection right, or the risks and harms of getting it wrong. The first stories were heard and seen in the videos and blogs produced for the project launch in May 2021. Why stories? First, because humans respond to stories, which connect us to each other in ways that data, information and other delivery methods do not. And second, because of the powerful "ripple' effect of trusted human-to-human contact, which can engage our emotions and drive positive behavioural change. If someone we know and trust tells us something, we are very likely to listen, to trust them, and to think about following the same course.

The Bijou project turns the conversation to the human, encouraging a sharing of information, support and advice, and a consequent mainstreaming of good data governance. The culture shifts as participants connect with their colleagues and share their values and behaviours. Stories that resonate with people can illuminate the fundamental principles of fair and lawful data processing, in a way that laws, policies and strategies - no matter how carefully crafted - cannot. The aim is to normalise privacy, data protection and ethics within the culture of the organisation.

The project particularly contemplates people who are dis-engaged from data protection. We know that many data breaches are accidentally caused by such persons and can be avoided by simple changes in approach. Similarly, many external hacks can be avoided by basic data hygiene inside the organisation. The people involved are not wilfully negligent but are unaware of the values at the heart of data protection, to protect the dignity of the individual and to prevent them suffering harms. Project Bijou empowers individuals to give their fellows the opportunity to understand what happens to personal data, and how their decisions and their practices can have an impact, not just on themselves but on others too.

Guernsey is a small community, where word of mouth can often have more of an impact than any marketing campaign, and is thus an ideal place to initiate the Bijou project. But it is none the less a test bed for a radical new tool in the accountability toolbox. It is a true accountability initiative, aimed at proactively changing the culture by influencing individual behaviour, rather than by simply enforcing compliance. It sends an original and powerful message to the global privacy community that education and training are not the only paths to accountability in the workplace.

See Bijou for yourself, together with the stories by local and international contributors at: https://www.odpa.gg/project-bijou/

CHRISTOPHER DOCKSEY

Honorary Director-General, European Data Protection Supervisor

Christopher Docksey was appointed as Honorary Director-General of the EDPS after serving as Director in charge of the EDPS Secretariat. He started his career as a law lecturer in the UK and the US before moving to the European Commission. As a member of the Commission Legal Service he was the Legal Adviser responsible for providing legal advice on data protection legislation, on negotiations on international data transfers, and for representing the Commission in the data protection cases heard before the European courts.

Since retiring from the EDPS he has been appointed as Member of the Data Protection Authority of Guernsey and as a Member of the Advisory Board of the European Centre on Privacy and Cybersecurity at the University of Maastricht. He has written numerous articles on privacy and data protection and is one of the authors and principal Editors (with Professors C. Kuner and L. Bygrave) of the Oxford University Press Commentary on the General Data Protection Regulation.

EMERGING PRIVACY REGIMES AND THE NEED FOR US LEADERSHIP IN THE DIGITAL ECONOMY

By Julie Brill, Corporate Vice President, Chief Privacy Officer, and Deputy General Counsel for Global Privacy and Regulatory Affairs at Microsoft

The European Union's Global Data Protection Regulation (GDPR) took effect on May 25, 2018, and since that day, the law has had a tremendous impact on the world of privacy. Indeed, it is not a stretch to call GDPR the most impactful global privacy development since Justice Brandeis' treatise on "The Right to Privacy", published 128 years earlier, at the end of the 19th century.

If we step back and look at how the world has changed since 2018, we see a rapidly evolving regulatory environment, one in which GDPR has become the de facto global standard for privacy. Several countries, including Brazil, Canada, China, India, Japan, New Zealand, South Korea, and Thailand, have passed or proposed new laws, or are considering changes to existing laws, that are inspired by GDPR. These countries and their domestic businesses are working towards meeting the adequacy standards set out by GDPR or renewing their adequacy status. This has led these jurisdictions and many others to more closely align with some of GDPR's strong protections.

For example, Brazil's data protection law became effective in 2020, bringing with it the creation of the Data Protection National Authority (ANPD), a new authority charged with building out the law's requirements through rulemaking. Inspired by the GDPR, the Lei Geral de Proteção de Dados Pessoais (LGPD) imposes new requirements on companies, government agencies, non-profits, and other organizations that use data in Brazil, offer goods and services to people in Brazil, or collect and analyze data tied to people in Brazil, regardless of where the organization is located. Similarly, in India we have seen legislators pursue the Personal Data Protection bill, with provisions inspired by GDPR, including requirements supporting individuals' control over their data, company accountability, and robust enforcement through a new data protection regulator.

In total, more than 130 jurisdictions around the world have enacted privacy laws.

In spite of all the activity to ensure that individual privacy is protected and companies are held accountable, there is a critical and noted absence: the United States. Home to nearly a quarter of the world's Fortune Global 500 companies and the headquarters of many of the largest technology companies, the United States does not have a comprehensive privacy law in place.

In contrast to the role it has traditionally played on global policy issues, the U.S. is not leading the discussion over privacy protections and common norms. The absence of U.S. action does not mean the absence of policy; instead, it means that the U.S. will continue to have little or no voice in the global conversation around what the rules of the road should be for American companies. That is a bad result for American businesses and organizations seeking to innovate and thrive in an ever-increasingly connected global economy.

These global laws are going to shape how the world adopts new technologies like artificial intelligence, biometrics, and ambient data collection through an ever-expanding Internet of Things. They are also going to help guide how we use technology and data to address some of the world's biggest societal challenges like climate change, racial inequality, and public health crises. The U.S. must enact a comprehensive privacy law in order to better protect people in the United States, and to join

the global conversations to shape this rapidly evolving landscape. It will be difficult for the United States to continue to argue for interoperable global standards that can improve innovation and benefit society when it doesn't have a comprehensive standard of its own.

If the United States doesn't enact privacy legislation soon, it risks seeing the balance of power on these issues shift away from Washington, D.C. to Brussels, New Delhi, and other capitals around the world that recognize the growing consensus that people's data must be handled with respect. There are new norms and rules coming to govern technology and data. The key question is whether the U.S. will have a hand in shaping them and defining the next wave of responsible innovation.

JULIE BRILL

Corporate Vice President, Chief Privacy Officer, and Deputy General Counsel for Global Privacy and Regulatory Affairs, Microsoft | Former Commissioner, US Federal Trade Commissioner

Julie Brill leads Microsoft's global privacy efforts and the team at the forefront of many of the regulatory issues that underpin the worlds digital transformation. As chief privacy officer at Microsoft, Julie serves as a global authority concerning policy and legal issues involving privacy; internet governance; telecommunications; accessibility; and corporate standards. In 2018, she spearheaded Microsoft's global adoption of the European Union's General Data Protection Regulation (GDPR), and now leads Microsoft's advocacy for complementary privacy mandates around the globe. Nominated by President Barack Obama and confirmed unanimously by the U.S. Senate, Julie Brill served for six years as a Commissioner of the U.S. Federal Trade Commission (FTC). As Commissioner, Julie worked actively on issues of critical importance to consumers, including privacy, fair advertising practices, fighting financial fraud, and maintaining competition in all industries, including health care and technology. While at the FTC, Julie was named "the Commission's most important voice on Internet privacy and data security issues," and one of the top four U.S. government players "leading the data privacy debate," among other honors. Julie has received numerous national awards for her work, including the New York University School of Law Alumna of the Year Award and most recently a Top Data Privacy Influencer of 2020. Julie graduated, magna cum laude, from Princeton University, and from New York University School of Law, where she held a Root Tilden Scholarship for her commitment to public service.

WELCOME DEVELOPMENTS IN DATA PROTECTION, BUT ARE THEY ENOUGH?

By Malcolm Crompton AM, CIPP, Founder & Lead Privacy Advisor, Information Integrity Solutions. Former Australia Privacy Commissioner

The rise of the digital age has profoundly changed the economics of personal data handling. The growing sophistication of data analytics coupled with data storage capabilities that would have been unthinkable a generation ago has created conditions that amplify the value of personal data to businesses. This has obvious implications for personal privacy because in the end, each data point is about a real live individual who deserves dignity, respect, and a rich personal life 'out of view'.

The problem we are faced with is this astonishing new data-driven business model is being regulated, in large part, by legacy privacy laws. Many such laws were either developed pre-internet or are based on laws that were. This includes the EU General Data Protection Regulation(GDPR). The result is a serious disconnect. Traditional privacy principles such as data minimisation and purpose limitation clash with new business imperatives that demand maximal data and unfettered data use and reuse.

And yet – with the usual lag between business innovation and regulatory reaction – we are beginning to see some changes in the regulatory landscape that demonstrate, if nothing else, that regulators and governments are actively grappling with this changed state of play.

First, there has been a conscious effort in more jurisdictions to expand the extra-territorial reach of privacy legislation, which Australia did 20 years ago. The trans-border operation of so many data-driven organisations has meant that data protection authorities have at times struggled to hold such organisations to account.

Second, there has been a trend for broadening the legal definition of personal data'. This enables privacy laws to regulate data (used in online tracking, profiling and targeted advertising) which might otherwise fall outside traditional definitions of personal data. The GDPR and California Consumer Privacy Act (CCPA) both offer examples of this.

Third, new and reformed privacy laws have strengthened regulator powers and increased the size of the penalties available to them. Several recent high-profile privacy cases have involved record-breaking fines. New laws – most notably the GDPR – have sought to enable imposition of fines that reflect the size and revenue of the tech giants and therefore better incentivise compliance. In other cases, particularly those involving the US Federal Trade Commission (FTC), we see record fines being imposed under existing laws.

Fourth, a number of jurisdictions have expanded the rights available to individuals under privacy law. The EU introduced a range of rights into the GDPR including the right to erasure (also known as the 'right to be forgotten'), the right to restrict processing, the right to object and rights associated with automated decision-making. The GDPR also gives individuals the right to withdraw consent at any time. Other jurisdictions have joined the EU in legislating the 'right to be forgotten', while California has given its consumers the right to demand that an organisation not sell their personal information.

Foundationally, such changes – the wider remit of privacy law, stronger regulator powers, and expanded individual rights – attempt to correct some of the power asymmetry between individuals on one hand, and tech giants and other data-driven organisations on the other. Nevertheless, the same intractable problems persist – the failure of the 'Notice and Consent' model wherever it is available, including in GDPR, limits of traditional privacy principles, the conundrum of data sovereignty, the inadequacy of consent buckling under the weight of overuse, and others. The recent developments outlined here are just a start and not enough.

In addition and notwithstanding the few significant examples of enforcement, the funding of privacy and data protection authorities worldwide is woefully inadequate almost without exception. Most organisations are 'getting away with it' most of the time including in Australia, Europe, the USA and elsewhere.

I believe that we are at a tipping point, by which I mean that we are at the point of engaging with those issues in new ways. We are already seeing how the lines are blurring between conversations about privacy, data sovereignty, AI, anti-trust and even democracy which creates fertile conditions for innovation in how we approach privacy.

My final observation is that there is nothing inevitable about the data-driven business model we are confronted with in 2021. This approach has been powered by two factors: obfuscation of how personal information is actually used (as so pungently described by the Australian Competition and Consumer Commission in its final report on its Digital Platforms Inquiry) and the innate human inability to assess, even in their own interests, short term gain versus long term loss. At last, the scale and impact of the long term losses such as insidious adverse discrimination and damage to democracy are becoming clear in the public mind.

In the same way as the world eventually learnt that the impact of ozone and now carbon emissions could actually endanger the planet, I am confident that the combination of economic pressure and regulation will develop the alternative for personal information and privacy. It will not be fast and it will not be easy, but it will happen.

MALCOLM CROMPTON

Founder & Lead Privacy Advisor, Information Integrity Solutions
Former Australia Privacy Commissioner

Malcolm Crompton is the founder, Lead Privacy Advisor and first Managing Director of IIS, with over 20 years' experience in privacy. As Australia's Privacy Commissioner from 1999 to 2004, Malcolm led the implementation of the nation's first private sector privacy law. He hosted the 25th International Conference of Data Protection and Privacy Commissioners in Sydney in 2003. Malcolm was the founding President of the International Association of Privacy Professionals Australia New Zealand (iappANZ), an affiliate of the US based International Association of Privacy Professionals (IAPP). He was a Director of IAPP from 2007 to 2011. He is a Director of Bellberry Limited, a private not-for-profit company which provides health ethics advisory services. He is also a member of the New South Wales Government Information and Privacy Advisory Committee, the State's Digital Identity Ministerial Advisory Council and the Palantir Council of Advisors on Privacy and Civil Liberties (PCAP), of Palantir Technologies.

Malcolm is a highly sought-after independent expert and has advised a wide range of industry sectors. This includes advising the Australian Bureau of Statistics on various matters (such as trust and social licence for the 2021 Census), a major Australian retailer on privacy issues on the horizon, Service NSW on its significant 2020 data breach, and the NSW and Victorian governments on their QR-code based COVID Safe check-in apps. He has also consulted to the Asia Pacific Economic Cooperation forum (APEC) regularly on implementation of the APEC privacy framework and to the Organisation for Economic Cooperation and Development (OECD).

INCREASING TRUST IN OUR DIGITAL SOCIETIES AND ECONOMIES: A KEY FACTOR TO IMPROVE PERSONAL DATA PROTECTION

By Dr. Eduardo Bertoni (PhD, Buenos Aires University) Representative, Inter American Institute of Human Rights | Former Director, Argentine Data Protection Authority

The pandemic caused by COVID 19 triggered many discussions about the benefits of "digital economies" and the mutation of our societies to what we can call "digital societies." In truth, these discussions were latent. The health emergency only accelerated processes that were already in the works. As an example, teleworking was possible before the pandemic, but it has since become necessary, and as time passed, it became more and more incorporated into our lives. Similar processes took place in areas such as "telemedicine," or meetings to discuss global issues that today can be done at low cost by convening people from different countries virtually.

All these activities involve in one way or another the use or processing of personal data. If such use or processing is carried out without rules that we trust will protect our privacy, we run the risk of losing the enormous opportunities that technology offers us today.

The question we must answer is whether the rules that exist today are, in the first place, sufficient to generate trust in users and if, thanks to that trust, they might be useful for the continuation and development of what we now accept as usual activities in these "digital societies".

My answer is regrettably that they do not.

The rules that exist today to protect personal data do not generate trust because they are not accepted globally. And this is a problem because personal data is constantly moving across country borders. Preventing this flow makes it impossible for activities of digital societies to occur.

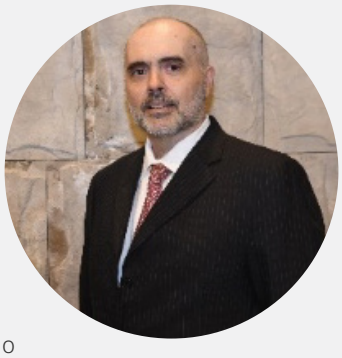
An important reason for the decrease in trust is that the lack of globalization of these rules prevents state entities in charge of protecting personal data -in the few cases that they exist and are independent- from enforcing their decisions. In other words, if a company is sanctioned in a country for violating data protection rules, it could evade the sanction for reasons of jurisdiction or applicable law. The consequence is that users in "digital societies" do not trust both in state institutions and rules that should protect them.

It is true that there are developments that can make us feel cautiously optimistic: the European Union's push for processes to adapt its own rules (the GDPR) or the Council of Europe's attempt to globalize Convention 108 are examples of measures that aim to globalize these rules. But, for instance, in Latin America there are very few countries considered to have adequate legislation or that are party to the Convention 108.

Consequently, one of the greatest challenges we face today is to work for an international treaty, with clear rules that can be followed in practice and enforced and ideally enforced globally. An agreement that brings States, companies, academics and users to the table for discussion is essential. Just as the pandemic accelerated the practices of the use of technology that were latent, the pandemic can also perhaps be a factor to accelerate the discussion and adoption of such a global agreement.

DR. EDUARDO BERTONI

Representative, Inter American Institute of Human Rights | Former Director, Argentine Data Protection Authority



Professor Eduardo Bertoni (PhD, Buenos Aires University) is currently the Representative of the Regional Office for South America of the Inter American Institute of Human Rights. He was the first Director of the Access to Public Information Agency (AAIP) which is the Argentine Data Protection and Access to Information Authority. He was the founder and the first director of the Center for Studies on Freedom of Expression and Access to Information (CELE) at Palermo University School of Law, Argentina. He was the Executive Director of the Due Process of Law Foundation (DPLF) until May, 2006. Previously, he was the Special Rapporteur for Freedom of Expression of the Inter-American Commission of Human Rights at the Organization of American States (2002-2005).

PRIVACY CULTURE AND CROSS-BORDER DATA TRANSFERS

By Stephen Kai-yi Wong, Barrister-at-Law | Former Privacy Commissioner, Hong Kong

"Those who assert the universality of human rights in the philosophical or an anthropological sense, focus on [sic] universal roots, however limited in number imprecisely expressed they may be. On the other hand, those who look for the human rights concept itself in all cultures inevitably conclude that the universality of human rights in this sense is a myth."[2]

In reality, there are different conceptions and regulations on human rights, including privacy, in different local jurisdictions, depending on their political structures, legal systems, histories, cultures and economic developments, etc. This is particularly true in terms of the applicability of the universality of human rights in jurisdictions which are not "western".

1. Arguably, the differences can be justified by the fact that state parties may opt in certain optional protocols and/or enter reservations or declarations when they become signatories of the international human rights instruments. One thing that is quite certain though, is namely all signatories intend to pursue and ultimately practise human rights protection acknowledged around the globe, their own interpretation of the universal standards and individual circumstances permitting.

2. Privacy and personal data protection regulations have been, and will continue to be, on the heels of technological development. While privacy protection has been strongly affected by technological development in a digital economy, privacy remains somewhat a culturally nuanced concept. The fragmented regulations around the globe in data protection in the 20th and the beginning of the 21st centuries did, in one way or another, expose the vulnerability of individuals' personal data protection and the associated misuse or abuse of their personal data by organisations, including the public authorities. The advancement of ICT developments, coupled with the increased awareness of the privacy right as a fundamental human right, has come to show that the "technology-neutral" and "principle-based" regulations are becoming unrealistic and outdated. It is no exaggeration to say that the implementation of the GDPR has brought about a mini-tsunami of privacy legislative reforms outside EU.

3. The demand for de-fragmented and stronger privacy protection regulations and enforcement is intensified by the surge of data-related crimes and cross-border transfer of data. Cross-border transfer of data may, in exceptional circumstances, act as facilitator of transnational data-related crimes. Where transnational data-related crimes have an impact on national security, the entire issues of personal data privacy protection, freedom of expression and other related human rights as enshrined in the international human rights instruments (many of which are incorporated in the constitutional documents of individual jurisdictions), as well as the balancing against the public interest, would be revisited, first within the local community and second in courts. Universality of privacy and other human rights will certainly be put forward as an argument but certainly no straight-jacket to resolving the issues.

1 *LL.M.(LSE), FHKIArb, QDR; stephenkywong@giltchambers.com*

2 *"Human Rights: Universality and Diversity", Eva Brems, Martinus Nijhoff Publishers, 2001, p.9*

4. Take the example of cross-border transfer of data between EU and other jurisdictions in the CJEU case of Schrems II[3]. The CJEU considering also the powers and functions of the US National Security Agency, found that US laws do not provide essentially equivalent data privacy right protection owing to the lack of proportionate governmental access to data and the appropriate redress for EU individuals in the US, mandated obligations to assess and verify the adequate protection in relation to, *inter alia*, "access by public authorities" of the importing jurisdiction.

5. It may not be fair to ask EU data exporters alone to assess the impact of, e.g. national security laws (and the related statutory exemptions and appropriate redress), of jurisdictions outside EU, in particular, where there are distinctly different jurisdictions and legal systems within one country, as in the case of Hong Kong *vis-à-vis* the mainland of China. This will inevitably place the dutiful responsibility on the data importer in Hong Kong to assist EU data exporter in assessing her compliance with the Standard Contract Clauses[4] (absent an EC Adequacy Decision). This assessment will also be part and parcel of verifying jointly whether Hong Kong is a jurisdiction equivalent to EU's in respect of, *inter alia*, data access by public authorities for the purpose of national security in the context of the recently implemented Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region effective 30 June 2020[5], as well as the related statutory exemptions and appropriate redress. All stakeholders have a significant role to play in constructing the "data travel bubbles", if not the universal privacy culture.

STEPHEN KAI-YI WONG

Barrister-at-Law, Hong Kong
Formerly Principal Government Counsel, Hong Kong (till 2014)
Formerly Privacy Commissioner for Personal Data, Hong Kong (till 2020)

Mr. Stephen Wong joined the then Attorney General's Chambers of the Hong Kong Government as a Crown Counsel in 1986 upon completion of the Government Legal Scholarship programme. He was appointed as the Privacy Commissioner for Personal Data of Hong Kong in August 2015. On top of overseeing a fair enforcement of data protection law, he allocated additional resources in education and publicity, and took the initiative to engage with the data-driven industry with a view to strengthening the culture of respecting individuals' personal data privacy, as well as maintaining a proper balance between free flow of information and data protection.

Mr. Wong completed his 5-year tenure as Privacy Commissioner in August 2020 and has since resumed private practice as a barrister-at-law in Hong Kong (www.giltchambers.com). He has since been developing a specialist practice in LawTech, FinTech and RegTech. His fields of legal practice, advocacy and advisory alike, also include issues relating to commercial law, trust, professional misconduct, and financial regulations and white-collar crimes. He is also active in education and community work, having been appointed as an adjunct professor of the Faculty of Law, Beijing Normal University and the School of Law, City University of Hong Kong; advocacy examiner of the Faculty of Law, University of Hong Kong; Honorary President of the Institute of Compliance Officers; Chairman of the Data Governance Certification Independent Vetting Committee of the Institute of Big Data Governance; and a member of the Advisory Board of Tencent Finance Academy (Hong Kong).

3 *See Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems and intervening parties, Case C-311/18*

4 *See Annex to the Commission Implementing Decision on standard contract clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, Brussels, 4.6.2021, C(2021) 3972 final; https://ec.europa.eu/info/sites/default/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf*

5 *https://www.elegislation.gov.hk/fwddoc/hk/a406/eng_translation_(a406)_en.pdf*

SOME THOUGHTS ON INFORMATION CLIMATE CHANGE

By Dr. Alexander Dix, LL. M. Vice-Chair of the European Academy for Freedom of Information and Data Protection. He was Data Protection and Freedom of Information Commissioner in Brandenburg (1998-2005) and Berlin (2005-2016).

Sir Bruce Slane, New Zealand's first Privacy Commissioner, at the end of his term of office in 2003 highlighted the importance of privacy by drawing a parallel to the air we breathe: both are invisible and we only notice it once it's gone. So when Scott McNealy said in 1999: "You have zero privacy anyway, get over it" he might as well have said: "You don't have any air to breathe, so just stop breathing." Twenty years later, Mark Zuckerberg uttered: "The future is private" (after taking the opposite view all along since setting up Facebook).

So are we witnessing a positive climate change with regard to privacy and data protection? Doubtless, there are some positive developments. Since the GDPR entered into force 2018, 17 more countries have adopted privacy laws and 163 more privacy tech vendors have started their businesses. However, some signs point in the opposite direction. Our informational and technological environment is changing at what the European Commission once aptly described "breakneck speed". Some have described this development as causing a "data tsunami".

Richard Thomas, then UK Information Commissioner, at the 2010 International Conference of Data Protection and Privacy Commissioners in Jerusalem, made a remarkable intervention during a panel on biometrics. At that time facial recognition technology started to become available, but Google had declared publicly that they would refrain from deploying facial recognition technology for ethical reasons. Thomas was skeptical as to how long this position would be upheld and urged the Commissioners to raise public awareness by pointing to the risks for women in particular if one day facial recognition would be rolled out for commercial use. Women being the majority of data subjects would form a strong opposition against the use of this technology that facilitates stalking (to name but one negative consequence).

More recently, while Microsoft and IBM have stopped the sale of facial recognition software to police departments in the US due to privacy concerns and the discriminatory effect of the software, and Amazon has extended its moratorium on police use of facial recognition "until further notice", two smaller companies are making the headlines. ClearView AI is offering the technology to local authorities and law enforcement agencies and this offer is being taken up by a number of US cities and the US Postal Service. On the other hand, half a dozen US states and several other cities have banned the use of the technology. The company PimEyes, initially launched by a Polish start-up, is offering facial recognition not only to public bodies but also the general public. PimEyes markets its service with a privacy spin: everyone should have the right – so they say – to find out where their photos have been posted online and get alerts when they are posted. PimEyes has become wildly popular among stalkers. Its general use would in effect be the end of anonymity and free movement in public places. As Stephanie Hare has rightly observed, while technical gadgets such as smartphones can be switched off or left at home, faces cannot. ClearView AI and PimEyes are now under investigation in Europe as to whether they comply with the provisions of the GDPR.

But the wider picture of our global informational ecosystem must include China where the government has declared it wants the country to be a world leader in artificial intelligence by 2030. Facial recognition is considered to be a helpful tool to identify people in mass gatherings in case there is "a major accident". The determination of what constitutes a major accident can be illustrated by recent events in Hong Kong. The official values and policy of the Chinese government are diametrically opposite

to what western democracies stand for. And still, even in the United States some Capitol rioters in January 2021 have been identified by private "sedition hunters" using PimEyes (which is currently legal in the U.S.).

The question we have to decide is: which kind of society we want wo live in? Technology is man-made, not a natural disaster like a tsunami (although some of these "natural" disasters are themselves man-made as a result of climate-change). Technology can and should be regulated. However, regulation very often comes too late to influence design decisions, business models and infrastructures. Regulation is necessary, but not sufficient.

What is needed, in addition, is twofold: raising the awareness of young people (even at kindergarten-level) for the fundamental importance of being let alone if they want to. And secondly a code of ethics for IT-engineers similar to the Hippocratic Oath for doctors is needed, supervised and enforced by professional bodies. Not every technology which is legal is ethically and socially acceptable. After all, the defense of privacy is too important to be left to Data Protection and Privacy Commissioners alone.

DR. ALEXANDER DIX

Vice-Chair of the European Academy for Freedom of Information and Data Protection in Berlin
Former Berlin Commissioner for Data Protection and Freedom of Information

Dr. Alexander Dix, LL.M. (Lond.) is Vice-Chair of the European Academy for Freedom of Information and Data Protection in Berlin. He has more than 30 years practical experience in Data Protection and Freedom of Information. From 1998 to 2005 he was Commissioner for Data Protection and Access to Information in Brandenburg. He was then elected as Berlin Commissioner for Data Protection and Freedom of Information, a post which he held until January 2016. From 2005 to 2015 he chaired the International Working Group on Data Protection in Telecommunications (also known as "Berlin Group") and represented the German Länder in the Art. 29 Working Party of European Data Protection Authorities. Currently he is a member of the Expert Group on Governance of Data and AI in the UN Global Pulse Project.

Dr. Dix has published extensively on transborder data flows, privacy in global networks and freedom of information. He was co-editor of the Jahrbuch für Informationsfreiheit und Informationsrecht (2008-2019) and is currently a member of the Editorial Board of the European Data Protection Law Review and the Editorial Advisory Board of the Journal International Data Privacy Law.

CAN DATA PROTECTION PRINCIPLES AND INNOVATION BE RECONCILED AND HOW?

By Yann Padova, Partner, Baker McKenzie | Former Commissioner, Commission de Régulation de l'Energie

If you search for the word "innovation" in the GDPR you might be disappointed. Indeed, you will find no occurrence at all. In our current digital world, this akin to an elephant in the room. Everybody sees that innovation is the driver of new services, a differentiator that ultimately has consequences on the growth of an economy. Everybody knows that most of the digital innovation relies on intense data processing. However, the most important piece of legislation on personal data in Europe is silent about it.

This silence is also supported by another debate about the need to encourage, if not require, companies to share data. Such claims focus on specific sectors such as environment, transportation, insurance and health or target specific actors, the GAFAM -- not to name them. The rationale for these claims is alternatively the alleged scarcity of available data that is believed to impair innovation or the concentration of data in the hands of a few dominant and gate-keeping companies that has the same effect.

In order to fight against these phenomena, the EU Commission contemplated in 2020, among other measures, the introduction of the notion of "data in the general interest", following the initiative taken by the French lawmakers in 2016. However, the legal validity of this new notion remains to be demonstrated. Besides, the legal ground for mandatory sharing proves itself to be challenging to establish in light of the value and the strength of the right of property. More recently, the EU Commission has introduced a draft regulation, the Digital Market Act, that targets the so-called gatekeeper companies and sets several obligations, in particular relating to the combination and the use of data.

Nevertheless, our point here is that these claims underestimate the importance of the systemic and legal conditions that are conducive to using data in order to foster innovation. Indeed, data innovation entails defining qualities that hardly cope well with some of the core principles of the GDPR. Data innovation, name it AI or "Big Data" a few years ago, is about trying to find correlation in massive and messy sets of data with unspecified *a-priori* purposes, learning algorithms that change depending on the data input and the output, reuse of data and combining it with other sources .... All these features enter in collision with some of the GDPR's fundamental principles such as data minimisation, purpose limitation, data retention, data accuracy to name a few. The tension is obvious and the focus on data sharing may be looking at the wrong side of the problem.

Indeed, is innovation just a question of access to massive volumes of data, or does it also – and above all – require a favourable and incentive-based legal framework? On the substance, the fact that data is scarce is debatable and to rely on this assumption favours "quantitative" criteria to the detriment of an analysis of the systemic and legal prerequisites conducive to innovation and competition.

British regulators have understood the complexity and the ambivalence of the links between innovation, competitiveness and data protection. They organized themselves in order to make innovation an instrument to strengthen companies'

competitiveness through the so-called "sandbox" technique[1], thereby demonstrating that the approach based on innovative uses of data is just as, if not more, important than the mere issue of access to data and data sharing. Such initiatives may be seen as an implicit acknowledgment that the interplay between the legal framework applicable to data protection and innovation is not, by design, necessarily and unconditionally favourable to innovation.

This need to organize a "safe space" for innovation has crossed the Chanel since the EU draft regulation on AI provides also for sandboxes. Maybe the GDPR creators should reflect on whether the current regulation strikes the right balance between innovation and data protection and provides the relevant tools to address the unprecedented challenges and opportunities of AI.

YANN PADOVA

Partner, Baker McKenzie

Former Commissioner, Commission de Régulation de l'Energie

Yann Padova joined Baker McKenzie as a partner in the Information Technology Group and head of the Data Protection Practice in Paris. He is internationally recognized in digital network law, personal data and regulatory law. Yann Padova has an extensive experience in data protection for 20 years and has served both as a regulator and a lawyer. In November 2017, he has been appointed "Country Leader" by the International Association of Privacy Professional (IAPP). Before joining Baker McKenzie, Yann Padova served as Commissioner with the Commission de Régulation de l'Energie (energy regulator 2015-2017), to which he was appointed by the President of the National Assembly due to his skills in the field of personal data and in light of the issues arising from the roll out of smart meters and smart grids in France. Before this, he had worked for Baker McKenzie in Paris as Senior Counsel in the Information Technologies and Communications team (2012-2015).

For 6 years, he was Secretary General of the CNIL, the French data protection authority (2006-2012) where he participated in the very first rounds of negotiations of the GDPR. He began his career as an Administrator (staff member) at the National Assembly (1995-2006) where he specialised in personal data law and criminal law and served at the Law Committee. He notably participated in the legal work that led to the transposition of the Directive 95/46 on data protection into French Law in 2004. Yann Padova teaches Data Protection regulations and laws at Paris II Law University (Assas) and at Sciences Po Paris. He is a member of the scientific council of the French legal review Lamy "droit de l'immatériel" (RLDI).He has published several articles in French and international legal reviews on topics such as the interplay between data ownership and data protection, big data and the GDPR, the territorial scope of the right to be forgotten or international data transfers.

1 *The Financial Conduct Authority (FCA) implemented the first "sandbox" in 2015. The ICO in turn committed to this approach in 2018.*

DATA IS A RAW MATERIAL, THE REGULATION OF WHICH STILL REQUIRES WORK

By Reijo Aarnio, Senior Adviser, Sitra | Former Data Protection Ombudsman, Finland DPA

Recital 2 of the EU's General Data Protection Regulation (2016/679, GDPR) contains one of the finest juridical ideas. The GDPR is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons. I would add to this the serving of people and quality of life, especially quality of life in the digital sphere.

Consent alone does not guarantee data-related balance

A human-centric data economy must not be based too much on consent "alone". More empowerment of data subjects is needed. Consent is an excellent juridical instrument, acknowledged also in the Charter of Fundamental Rights of the European Union as a key basis for the processing of personal data. Consent is a unilateral expression of intent indicating a person's data-related right of self-determination and thus it differs from a contract, for example.

Naturally, consent requires that the party requesting it acts according to consent-related statutory requirements. After receiving consent, the data controller must adhere to it and also accept that consent can be withdrawn unilaterally. Does consent oblige the data controller to actively take action, such as share personal data?

The GDPR gives the data subject a new right – the right to data portability (GDPR, Article 20). Recital 68 describes this right and provides grounds for it: the need to further strengthen the data subject's control over his or her own data and his or her right to transmit it to another controller. According to this recital, this right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract.

The structure has some essential deficiencies. First of all, the regulation also contains other legal bases for processing other than consent or a contract. The GDPR does recognise the data controller's legitimate interests. Why couldn't the data subject's legitimate interests also constitute a right that enables the exercise of their data-related right of self-determination? The right to rectification, the right to be forgotten, the right to object to the processing of personal data and the right to restrict processing do not, as such, offer sufficient means to exercise this data-related right of self-determination.

Furthermore, the right to data portability does not apply to personal data in the possession of the public sector, although data portability should be part of the principle of service that is an element of good administration. As a result, no fair data-related balance has emerged between data controllers and data subjects and consumers have not had the opportunities to take part in competitive tendering among service providers within the internal market, to gain a better freedom of choice or to reap product- or service-related financial benefits.

The individual may not be left alone

Where does this concern stem from? While data is being described as "the new oil" or another business raw material, we should understand that it is actually the only raw material for which its use is not regulated in a satisfactory manner.

The best-case scenario is that regulation is global and based on human rights. Luckily, we at least have the GDPR, which strengthens this value base and binds data-related rights to fundamental and human rights. However, at the same time, transnational digital giants continue to dictate the terms, conditions and methods of data use, outside the scope of the parliamentary system. The individual has been left quite alone against them.

Data protection is a freedom that should be defended

When it comes to the use of the digital raw material, or our personal data, problems with consumer protection and competition law have also been identified. An illegal dominant position in the market may be based on personal data.

I have been delighted to notice that the protection of personal data and sustainable development, an absolute necessity for the environment, have approached each other. Data protection is related to the energy economy, mobility and traffic, smart homes and many other phenomena that can, at their worst, challenge ecological resilience and climate.

For its part, data protection also protects the fairness of our election systems and, consequently, the whole of democracy. Indeed, the protection of privacy has sometimes been defined as the right to mind one's own business and to form opinions without the intervention of others. Data protection is a freedom that should be defended.

New business models challenge data policy

Business models have changed, too. They have moved from direct customer relationships through value chains to entirely new ecosystems that are based on data sharing. The consumer must be reinstated as the king of this hill and provided with more power over the use of their personal data.
Luckily, the European Union and many of its individual member states have started to react to this situation. We can expect a whole new wave of legislation. It will force the member states to consider the quality of their data policies and their role in societal decision-making.
What about business operators and the third sector? They must not be left alone in the midst of this difficult-to-grasp transformation. By supporting them, we will also support the realisation of the recital I quoted at the beginning of this text.

Digital sovereignty

In conclusion, it is good that we have woken up to cybersecurity. Now we also need to be awakened to the need to strengthen a human-centric, fair data economy and the right of digital self-determination (digital sovereignty).

My theses – what we need is:

1. a human-centric future that is based on a stronger data-related right of self-determination;
2. stronger digital sovereignty and decision-making that respects human rights; and
3. more comprehensive and democratic global regulation of "digital natural resources".

REIJO AARNIO
Senior Adviser, Sitra
Former Data Protection Ombudsman, Finland DPA

Mr. Reijo Aarnio (born 1955) graduated from the University of Helsinki, Faculty of Law in 1981. He then worked at several expert and managerial tasks in the private sector and aided the committee drafting the Personal Data Act in an expert capacity. In 1997 Reijo Aarnio became Data Protection Ombudsman. He retired in October 2020. The Data Protection Ombudsman is appointed for a term of five years or less at a time. Since November 2020 has been working as a Senior Advisor of The Finnish Innovation Fund Sitra focusing on matters of democracy, health data and fair data economy. Mr. Aarnio has lectured in the Universities of Helsinki, Lapland and Georgetown. He has been an adjunct Professor of Law at Georgetown University. He has been a member of the Steering Group of Information Security in State Government, National Information Security Advisory Board, permanent expert in an governmental information society programme (2003-2007), the Ministry of Social Affairs and Health working group on labour issues, Joint Supervisory Authority of Schengen, Joint Supervisory Body and Appeals Committee of JSB of Europol and Article 29 Data Protection Working Party, later European Data Protection Board, since 1997, vice chairperson of the Working Party from 2000 to 2004. Has has been a permanent expert collaborator of the European Commission in the projects (Twinning and PHARE) addressed to candidate countries and new members, in the field of data protection. He cooperated also with the EU Council chairing the Schengen Evaluation Team focused on new members states. He was appointed by the European commission as a member of the Expert group on credit histories. He was a member of Council of Human Rights in Finland from 2012 to 2020. He has also been a Head of Editorial Board of Data Protection Magazine and a regular blogger.

ACCOUNTING FOR WOMEN'S DIFFERENT EXPERIENCES WITH PRIVACY ONLINE

By Emily Sharpe, Director of Policy, The Web Foundation

In 1989, Sir Tim Berners-Lee was working as a software engineer at CERN, the large particle physics laboratory in Switzerland. Throughout his tenure at CERN, he noticed that the scientists who had come from all over the world to use its accelerators were having difficulty sharing information.

"In those days, there was different information on different computers, but you had to log on to different computers to get at it. Also, sometimes you had to learn a different program on each computer. Often it was just easier to go and ask people when they were having coffee..." Tim has said.

Tim saw a way to solve this problem. Already, millions of computers were being connected together through the fast-developing internet, and he realized they could share information by using an emerging technology called hypertext.

In March 1989, Tim set out his vision for what would become the web in a document called "Information Management: A Proposal." Fast forward to the end of 1990, and the first web page was served on the open internet.

The web quickly became a place for global innovation and collaboration never seen before. It created opportunity, gave marginalized groups a voice, and made our daily lives easier. The Covid-19 pandemic has shown us that the web is a lifeline, not a luxury. But access to these digital spaces is not equal for everyone. Thirty years on from the invention of the web, only half of the world was able to connect. And for those who are online, too often they are driven offline by privacy violations, online harassment, censorship, fraud, and more.

In 2009, Sir Tim co-founded the World Wide Web Foundation with Rosemary Leith to address these challenges and to galvanize the global community to fight for the web we want: a web that is safe, empowering, and genuinely *for everyone*.

Today the Web Foundation continues to fight for digital equality and opportunity, with a special focus on half the world's population: women. Our recent research on women's rights online highlights the stark gaps between how women and men experience the web and digital services, with men 21% more likely to be online than women, rising to 52% in the world's least developed countries. There are also gaps in quality of connectivity and digital skills, and threats that disproportionately impact women's privacy and safety — all of which prevent women from fully benefiting from the opportunities that digital technology offers.

Our research shows that women on average have lower levels of trust in private companies, with 54% stating they would not allow companies to use any of their data, compared to 47% of men. Women are more concerned than men about the privacy of their personal data, such as private messages, personal data of family members, medical records, and home addresses.

And women are more concerned about the potential harms they face if their information is misused. Women are disproportionately affected by serious privacy violations in some areas, like doxing, the sharing of non-consensual images, cyberstalking, and surveillance via connected devices by abusive partners.

Our survey also found women are less likely to be creators of content when they do get online. Men were far more likely to engage in a range of online activities, including posting comments about political, social or economic issues, selling products or advertising a service, or publishing a blog post. There needs to be more research into the reasons behind this gap — including the role privacy concerns play in women's lower levels of content creation.

There is no "universal" experience of the web. We must recognize that individuals' gender, race, ethnicity, socio-economic class, sexual orientation, and other intersecting and overlapping identities impact how they perceive, interact with, and are served by data, products, and policies. The global tech community must adopt a more intersectional approach to developing policies and products that account for the full diversity of those who use digital tools, especially from a privacy and data protection perspective. As a starting point, companies, governments and researchers should collect gender-disaggregated data around women's and men's perceptions of privacy and use of data-driven services.

EMILY SHARPE
Director of Policy, World Wide Web Foundation

Emily Sharpe serves as Director of Policy at the World Wide Web Foundation. In this role, she is responsible for developing the Foundation's policy positions and goals, and for leading advocacy engagement as we aim to ensure that everyone, everywhere can access the free and open web.

Prior to joining the Web Foundation, Emily led Facebook's privacy policy engagement team in Europe, Middle East and Africa. Trained as a human rights lawyer, she has held legal, policy and research positions with a number of NGOs, human rights law practices and public bodies. Emily earned her law degree from the Georgetown University Law Center and her undergraduate degree from Cornell University, and was awarded a Fulbright scholarship to Qatar and Kuwait.

GOVERNING FOR PRIVACY AND OTHER DEMOCRATIC GOALS

By Peter Swire, Professor and Associate Director, Georgia Tech

Along with other contributors to this symposium, I have devoted much of my professional life to privacy protection. Throughout my quarter-century in the privacy field, one recurring issue has been what sorts of institutions can serve privacy, while also meeting the other goals that any society has. In the language of Article 8 of the European Convention on Human Rights, how might we best protect privacy while recognizing other interests that are "necessary in a democratic society"? The interests listed in Article 8 would seem vital to consider, whatever one's view of politics or the just society. They are "national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

One conundrum is how close the privacy official should be to the other organs of government. If the privacy official (or institution) is entirely part of the executive branch, then the fear is that the other interests will overwhelm the privacy voice. On the other hand, if the privacy officials are entirely outside of government, then those officials may lack information or experience about what actually is "necessary in a democratic society."

Under the European Charter of Fundamental Rights, "independence" is the principle answer. Compliance with data protection "shall be subject to control by an independent authority." (Art. 8) In addition, for a claimed violation of rights, everyone is entitled to a hearing "by an independent and impartial tribunal." (Art. 47)

There are compelling arguments to support such independence. Enforcement actions should be brought without favoritism. Judges should be impartial and not subject to political coercion. In addition, there is the often well-founded concern about agency "capture" – the concern that that the regulated actors will gain too much influence over decisions of the regulators.

With that said, it is deeply educational for a privacy regulator to experience being subject to privacy requirements. While I served in the White House under President Clinton, we required each agency to have a privacy policy clearly posted on its website, and worked hard to ensure compliance. Then, at a Congressional hearing, the political opposition discovered one tiny agency that we frankly had never heard of. It lacked a privacy policy, and the headlines shouted that the government was breaking its own rules. Later, when drafting the U.S. medical and financial privacy rules, one priority was to consider which requirements could actually be implemented in practice.

"Insider" experience is especially important for national security and other topics that are not readily accessible to privacy generalists. In 2013, I served on the NSA Review Group, tasked by President Obama to recommend changes after the Snowden revelations. Two of the other members had terrific knowledge of actual practice, as former anti-terrorism advisor to the President and former Director of the CIA. As the privacy lead, I suggested numerous possible reforms. So did Geoffrey Stone, who had long been a leader of the American Civil Liberties Union. When we proposed something that the insiders said was workable, then we had far greater confidence that the reform would meet the multiple goals of a democratic society, including national security and also fundamental rights.

Based on these experiences, there is reason to be cautious if authoritative interpretations of rules about data are issued by actors whose sole or primary task is to seek stricter privacy protections, to the exclusion of other goals such as national security or economic growth. As the EU seeks its own answers on such challenging questions, two institutional approaches have relatively greater experience in valuing privacy as well as other concerns. The first are those agencies complying with the Law Enforcement Directive. Similar to my own time in government, government experts there are tasked to protect privacy while also being subject to privacy requirements. That insider perspective may suggest approaches that are both workable and privacy protective.

The European Court of Human Rights (ECtHR) is a second source of expertise. In contrast to the Court of Justice of the European Union, with its jurisdictional limits on national security, the ECtHR for decades has been tasked with protecting privacy as well as national security and other values. The ECtHR has continued to provide governments a "margin of appreciation" on national security issues, in part justified by the fact that the judges are not fully briefed on the actual dangers, and the possibility that such dangers to survival of the society may change quickly.

All of us in the privacy field seek wisdom in how to uphold fundamental privacy rights while also preserving the full range of democratic values. It is risky for decisions important for national security to be made by those who lack access to classified materials. It is also risky to let national security officials make these decisions unchecked. As all democracies face the challenge of governing data in a data-based society, I hope readers will consider what mix of insider knowledge and independence will serve us best.

PETER SWIRE
Professor and Associate Director, Georgia Tech

Peter Swire is the Elizabeth and Tommy Holder Chair of Law and Ethics at the Georgia Tech Scheller College of Business, where he teaches privacy and cybersecurity. He is senior counsel with Alston & Bird LLP, and Research Director for the Cross-Border Data Forum. In 2015 the International Association of Privacy Professionals awarded him its Privacy Leadership Award. In 2013, he served as one of five members of President Obama's Review Group on Intelligence and Communications Technology. Under President Clinton, Swire was the Chief Counselor for Privacy, in the U.S. Office of Management and Budget, the first person to have U.S. government-wide responsibility for privacy policy.

WHAT IS "DATA ETHICS," AND WHY IS IT IMPORTANT?

By Dennis D. Hirsch, Professor of Law, The Ohio State University Moritz College of Law and Capital University Law School

f you are a sentient being and are at all involved in the field of privacy, you have no doubt heard about "data ethics." You may also have wondered: "what does this term really mean" and "how do organizations achieve it on the ground?" I had these questions and they led me, several years ago, to initiate a research study of what companies do when they pursue data ethics. I was lucky enough to convince Ohio State colleagues from the fields of business, computer science, philosophy and sociology to join me in this exploration. Combined with my own field of law, this multi-disciplinary team was able to examine data ethics from multiple perspectives. We interviewed twenty-three leading practitioners of data ethics and surveyed fifty more. Here is some of what we learned.

First, the field of data ethics in its recent incarnation is a response to the growing use of advanced analytics and artificial intelligence, and the risks that these technologies pose to individuals and the broader society. These risks include not only violations of privacy but also bias, manipulation, opaque "black box" decision-making, entrenchment of inequality, undermining of democracy and other potential harms.

In the past, organizations whose use of data posed risks to others sought to address this by complying with privacy laws and the fair information practices (FIPs). But the companies we talked to explained that, when it came to advanced analytics and AI, this strategy was woefully insufficient. For one thing, advanced analytics and AI pose risks that go well beyond privacy to bias, manipulation, etc. For another, privacy law's central tools – notice, consent and purpose limitation – don't protect people who cannot understand what data scientists can infer from their data, and so cannot make meaningful choices about whether to share this data in the first place. Privacy law remains vital, even essential. However, it does not protect people from the harms that advanced analytics and AI can create.

To reduce these risks, the companies said that they had to go beyond privacy law and the FIPs. They had to try and spot bias and fix it; distinguish between persuasion and exploitation, and stop themselves from engaging in the latter; find ways to make their algorithms more explainable and less opaque; and to take other such steps that privacy law does not require. As they put it, they had to go beyond the law and into the realm of "ethics." For them "data ethics" does not mean aligning their operations with one ethical philosophy or another. It means going beyond legal requirements to reduce risk to individuals and the broader society.

This formulation demystifies data ethics. It takes it out of the realm of philosophy and puts it squarely into that of beyond compliance business behavior. Thoughtful companies know how to go beyond compliance. They have done it in the environmental and worker safety areas. Now they need to do it for advanced analytics and AI.

This begs the question of why a company would do more than what the law requires it to do. Here, too, the answers are not mysterious and hew closely to the reasons why companies pursue self-regulation generally. Some do it because a founder or CEO instilled core values that the company wants to honor. But most do it because they believe it enhances their competitiveness and bottom line. Companies pursue data ethics to avoid incidents like the Facebook-Cambridge Analytica scandal, preserve

their reputations and sustain their trusted relationships. They seek to achieve data ethics because they know that regulation of advanced analytics and AI is coming. The European Commission's recent proposed Regulation Laying Down Harmonized Rules on Artificial Intelligence, and the FTC's recent blog post on Aiming for Truth, Fairness and Equity in Your Company's Use of AI, demonstrate this. Companies want to get ahead of, and perhaps shape, this coming regulation. They practice data ethics so that they can better recruit and retain the young data scientists that are key to their business success and that want to work with companies whose values they share.

How do companies achieve data ethics? This brief essay cannot describe our findings on this topic. For that, I refer you to our research team's report: "Business Data Ethics: Emerging Trends in the Governance of Advanced Analytics and AI." I hope that you find the report to be useful and would welcome your feedback on it. Contact me at Hirsch.151@osu.edu.

DENNIS HIRSCH
Professor of Law & Director of the Program on Data and Governance, The Ohio State University Moritz College of Law

Dennis Hirsch is Professor of Law and Director of the Program on Data and Governance at The Ohio State University Moritz College of Law. He also holds the title of Professor of Law at Capital University Law School. Professor Hirsch's research interests lie at the intersection of governance theory and information privacy law and he has written extensively in this area. He also writes about European data protection law, comparative information privacy law, and the instructive similarities between environmental law and privacy regulation.

In 2010, he served as a Fulbright Senior Professor at the University of Amsterdam where he produced a leading study on collaborative Dutch data protection regulation. Professor Hirsch has published articles in the Illinois Law Review, the Georgia Law Review, the Indiana Law Journal, the Administrative Law Review and numerous other law journals. He is the co-author (with Jerry Anderson) of Environmental Law Practice: Problems and Exercises for Skills Development (Carolina Academic Press), a textbook adopted at over thirty law schools. He teaches courses on Information Privacy Law, Big Data Law and Policy, and Environmental Law.

NEUROTECH AND PRIVACY OF THE MIND

By Dario Gil, Senior Vice President and Director of IBM Research

The next 10 years will bring about all manner of revolutionary data-driven technologies that pose both tremendous benefits and alarming privacy risks. Of these, neurotechnology, or neurotech, will likely be one of the most disruptive.

Neurotech is our, frankly, mind-blowing attempt to connect human brains to machines. Although brain-computer interfaces (BCIs) are the heart of neurotech, it is more broadly defined as technology able to collect, interpret, infer or modify information generated by any part of the nervous system. Why? To develop therapies for mental illnesses and neurological diseases. Beyond health care, it could soon be used in education, gaming, entertainment, transportation and so much more.

But there are pitfalls: there are no widely accepted regulations or guardrails yet when it comes to neurotech's development or deployment. We must have principles and policies around neurotech, technology safeguards, and national and international regulations.

Neurotech is far from just conceptual -- such technology has already improved the quality of life and abilities of people with different illnesses or impairments, from epilepsy to Parkinson's Disease to chronic pain. One day, we might implant such neurotech devices into paralyzed humans, allowing them to easily control phones, computers and prosthetic limbs—with their thoughts alone. In 2017, Rodrigo Hübner Mendes, a paraplegic, used neurotech to drive a racecar with his mind. Recently, an invasive neurotech device accurately decoded imagined handwriting movements in real time, at a speed that matched typical typing. Researchers have also showed how invasive neurotech allows users with missing or damaged limbs to feel touch, heat and cold through their prostheses.

Emerging applications of neurotech provide even more promise. Not only can neurotechnology sense or read neurodata but it can also modulate—invasively and noninvasively. This research is still in early stages, but it's advancing rapidly. One astounding example is the work of Rafael Yuste, a neurobiologist at Columbia University. His team has recorded the neuron activity of a mouse that was performing an action, such as licking, for a reward. Later the researchers reactivated these same neurons and got the mouse to perform the same action, even if the rodent did not intend to do it at that moment. It is easy to imagine how this technology could lead to new breakthrough treatments for people with physical disabilities, for example.

Neurotech is still extremely immature. As it becomes more commonplace, we must consider the risks it might present, the ethics around it, and what regulation would be appropriate. Such risks are indeed vast, in some cases challenging the very autonomy of our own actions and the privacy of our thoughts. What if someone were to face employment discrimination because the algorithms that power a neurotech application used for hiring misinterpreted their neurodata? What if someone's most sensitive and private thoughts were shared without their knowledge or consent? Of particular concern is the fact that most of the neurodata generated by the nervous systems is unconscious, meaning it could be possible for users to unknowingly or unintentionally share sensitive neurodata. The presumption of privacy within one's own mind may simply no longer be a certainty.

While it is too early to know how to answer the questions neurotech poses about privacy and ethics, we need to ensure that researchers, corporations, policymakers, and consumers alike study and monitor this technology carefully. Developers of neurotech in particular must reaffirm their commitment to responsible innovation and help to develop and enforce guardrails so that they lead to beneficial long-term outcomes for the economy and society alike.

DR. DARIO GIL
Senior Vice President and Director of IBM Research

Dr. Darío Gil is Senior Vice President and Director of IBM Research. As a technology and business leader, Dr. Gil is responsible for IBM Research, one of the world's largest and most influential corporate research labs, with over 3,000 researchers. He is the 12th Director in its 76-year history. Dr. Gil leads the technology roadmap and the technical community of IBM, directing innovation strategies in areas including hybrid cloud, AI, quantum computing, and exploratory science. He is also responsible for IBM's intellectual property strategy and business. Dr. Gil is a globally recognized leader of the quantum computing industry. Under his leadership, IBM was the first company in the world to build programmable quantum computers and make them universally available through the cloud.

THE U.S. URGENTLY NEEDS A COMPREHENSIVE PRIVACY LAW THAT GOES BEYOND THE FAIR INFORMATION PRACTICES

By Woodrow Hartzog, Professor of Law and Computer Science, Northeastern University & Neil Richards, Koch Distinguished Professor in Law, Washington University in St. Louis

America's privacy bill has come due. Since the dawn of the Internet, Congress has repeatedly failed to build a robust identity for American privacy law. But now both U.S. states like California and the European Union have forced Congress's hand by passing legislation like the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). These data protection frameworks, structured around principles for Fair Information Processing called the "FIPs," have industry and privacy advocates alike for a "U.S. GDPR." States seemed poised to blanket the country with FIP-based laws if Congress fails to act. The United States is thus in the midst of a "constitutional moment" for privacy, in which intense public deliberation and action may bring about constitutive and structural change. And the European data protection model of the GDPR is ascendant.

But there are great risks of U.S. lawmakers embracing a watered-down version of the European model as American privacy law enters its constitutional moment. European-style data protection rules have undeniable virtues, but they won't be enough. The FIPs assume data processing is always a worthy goal, but even fairly processed data can lead to oppression and abuse. Data protection is also myopic because it ignores how industry's appetite for data is wrecking our environment, our democracy, our attention spans, and our emotional health. Even if E.U.-style data protection were sufficient, the United States is too different from Europe to implement and enforce such a framework effectively on its European law terms. Any U.S. GDPR would in practice be what we call a "GDPR-lite."

Our argument is simple: In the United States, a data protection model cannot do it all for privacy, though if current trends continue, we will likely entrench it as though it can. We propose instead a more comprehensive approach to privacy that is better focused on power asymmetries, corporate structures, and a broader vision of human well-being. Settling for an American GDPR-lite would be a tragic ending to a real opportunity to tackle the critical problems of the information age.

If you look closely, the foundation for a pluralistic American theory of privacy based upon constraining corporate power and protecting vulnerable consumers has already been established. We must embrace it. Practically speaking, lawmakers, courts, and companies must embolden the doctrines and legal tools that advance this agenda. This means strengthening trust-based torts like the breach of confidence and theories of indirect liability, prohibiting more data practices outright, and being more skeptical of the role of consent in validating data practices. It also means both governments and organizations must leverage the concept of privacy to further the over-all well-being of their citizens and customers. An effective approach to privacy also requires a shift from focusing mainly on procedural rules to include substantive restrictions as well. Procedural requirements like obligations to get peoples' consent for data practices ultimately normalize the kinds of data collection and surveillance harms that they are supposed to mitigate. They are a recipe for companies to exploit and manipulate people in service of ever more data. The substantive shift we call for will require lawmakers to revisit some basic assumptions about when data collection and processing is desirable and entertains bolder obligations, such as outright bans and moratoria on certain technologies and practices. It also requires legislatures to be imaginative and go beyond the standard suite of procedural safeguards like transparency and data subject rights like access to data. Lawmakers have been remarkably creative in creating rules for other industries. They should leverage the power to tax, change business incentives, and pierce the corporate veil in going beyond standard data and consumer protection approaches to confront modern privacy risks.

If the United States is to take the modern privacy dilemma seriously, lawmakers must act urgently and be willing to expend political capital for effective rules. America's privacy reckoning is here, but its identity has yet to be defined. Congress has an opportunity to show leadership by embracing a comprehensive approach that addresses modern data and privacy problems, not those of the 1970s. But if it fails to embrace a comprehensive framework that addresses corporate power, vulnerabilities in information relationships, and data's externalities, America will be resigned to a weak and myopic approach as its constitutional moment passes. Settling for an American GDPR-lite would be a tragic ending to a real opportunity to tackle the critical problems of the information age.

WOODROW HARTZOG

Professor of Law and Computer Science at Northeastern University School of Law and the Khoury College of Computer Sciences

Woodrow Hartzog is a Professor of Law and Computer Science at Northeastern University School of Law and the Khoury College of Computer Sciences. He is also a Faculty Associate at the Berkman Klein Center for Internet & Society at Harvard University, a Non-resident Fellow at The Cordell Institute for Policy in Medicine & Law at Washington University, and an Affiliate Scholar at the Center for Internet and Society at Stanford Law School. His research on privacy, media, and robotics has been published in scholarly publications such as the Yale Law Journal, Columbia Law Review, and California Law Review and popular publications such as The New York Times, The Washington Post, and The Guardian. He has testified multiple times before Congress and has been quoted or referenced by numerous media outlets, including NPR, BBC, and The Wall Street Journal. He is the author of Privacy's Blueprint: The Battle to Control the Design of New Technologies, published in 2018 by Harvard University Press. His book with Daniel Solove, Breached!: Why Data Security Law Fails and How to Improve It, is forthcoming with Oxford University Press.

NEIL RICHARDS

Koch Distinguished Professor in Law; Director, Cordell Institute, Washington University in St. Louis School of Law

Neil Richards is one of the world's leading experts in privacy law, information law, and freedom of expression. He writes, teaches, and lectures about the regulation of the technologies powered by human information that are revolutionizing our societies. Professor Richards holds the Koch Distinguished Professor in Law at Washington University School of Law, where he co-directs the Cordell Institute for Policy in Medicine & Law. Professor Richards serves on the board of the Future of Privacy Forum, is a member of the American Law Institute, and is also a consultant and expert in privacy cases. He is the author of Why Privacy Matters (Oxford Press 2021) and Intellectual Privacy (Oxford Press 2015). His many other scholarly and popular writings on privacy and civil liberties have appeared in wide a variety of media, from the Harvard Law Review and the Yale Law Journal to The Guardian, WIRED, and Slate. Professor Richards graduated in 1997 with graduate degrees in law and history from the University of Virginia, and served as a law clerk to both William H. Rehnquist, Chief Justice of the United States and Paul V. Niemeyer, United States Court of Appeals for the Fourth Circuit.

CHARTING THE LANDSCAPE FOR DATA PROTECTION & INTERMEDIARY PUBLISHERS

By David Erdos, Faculty of Law, University of Cambridge

At least in Europe, the basic data protection framework coalesced during the 1970s and very early 1980s. Even then, it was framework under serious socio-technological challenge. But since this time our experience of the gathering and spread of personal data through computerized networks has radically altered. One such change concerns the large-scale online spread of third-party personal data, which is promoted, organised, aggregated and rendered searchable by public dissemination services. These intermediary publishers include both generalist and specialised search engines, social networking sites and wide range of other online platforms. Huge conundrums present themselves as to whether and, if so, what data protection duties these services are subject to as a result of this personal information dissemination. Whilst Data Protection Authorities (DPAs) have grappled with such questions over many decades, it was the Court of Justice of the EU's decision in Google Spain that brought it to wide public attention. *Google Spain* memorably found that, at least in relation to name-based searches, a generalist search engine would need respond *ex post* to claims to deindex personal data whose processing would otherwise violate data protection norms. More abstractly, the Court specified that

> *Inasmuch as the activity of a search engine is ... liable to affect* ***significantly and additionally*** *compared with that of the [original] publishers ... the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its* ***responsibilities, powers and capabilities****, that the activity meets the requirements of [data protection].*

As my own work has explored, it is concerning that these tests don't seem to be present in the actual legislative framework which the Court said it was applying. European data protection has generally adopted a "processing" model which holds an operator responsible in any case where they are determining purposes and means, irrespective of whether the activity is significantly or additionally impactful. Moreover, the idea of removing duties on the basis of a lack of capability (or even power) in the relevant systems would appear in tension with the general expectation (now explicitly stated in laws such as the GDPR) that controllers should proactively ensure data protection by design. Nevertheless, the tests themselves may be considered quite reasonable and, aside from where services are clearly operating on behalf of another named or traceable entity which can realistically be held legally accountable, should be broadly applied. Nevertheless, not only is there a need to place this all on a statutory footing, but these abstractions clearly also require considerable further contextual specification. Thus, whilst Google and general search engines have accepted that nominative searches significantly and additionally affect data subject rights, what about searches based on an image, telephone number or job title and workplace? Should the functionality of social networking sites be considered intrinsically significantly and additionally impactful or, if not, how should in-scope processing be demarcated there? Finally, what can be done to ensure that action is respectful of users' enjoyment of freedom of expression, without fundamentally undermining these personal information safeguards? Related questions are being addressed in a wider range of legal contexts as the European Commission's draft Digital Services Act and the UK Government's Online Safety Bill highlight. The development of data protection should, therefore, take full account of these related developments. Only by legislators themselves addressing these issues in earnest can we hope that the landscape in this area might be effectively charted to the potential benefit of legitimate services, users and data subjects alike.

DAVID ERDOS

Deputy Director, Centre for Intellectual Property and Information Law (CIPIL), Cambridge University

David Erdos is Deputy Director of the Centre for Intellectual Property and Information Law (CIPIL) and University Senior Lecturer in Law and the Open Society in the Faculty of Law and also WYNG Fellow in Law at Trinity Hall, University of Cambridge. Before joining Cambridge in October 2013, David spent six years as a research fellow at the Centre for Socio-Legal Studies, Faculty of Law and Balliol College, University of Oxford. David's current research explores the nature of data protection especially as it intersects with the right to privacy, freedom of expression, freedom of information and freedom of research. In addition, David continues to have a research interest in bill of rights and related constitutional developments, especially in the UK and other 'Westminster' democracies. He has published a number of research articles in leading legal, sociolegal and political science journals and is the author of two OUP monographs, Delegating Rights Protection (2010) and European Data Protection Regulation, Journalism, and Traditional Publishers (2019).

HOW DO WE BALANCE PROSPERITY AND PROTECTION, ESPECIALLY IN INNOVATIVE AREAS?

By Professor Christopher Hodges OBE, Professor of Justice Systems, Centre for Socio-Legal Studies, University of Oxford

In simple terms, the purpose of business is to promote prosperity. It does this through creating and selling products and services in markets to people who find them useful. The justification for business goes through cycles of theory and policy, influenced by political ideology and public sentiment depending on events and the social context. One theory is that the purpose of business is solely to make profits, and that profits trickle down to deliver social good like employment, innovation and lifting people out of poverty. This is strongly associated with a political ideology that individuals and markets should be free. The argument goes that markets are always right, self-police, and need no intervention from the state through regulation, in the same way that individuals should be allowed personal freedom. After all, capitalism defeated communism, didn't it? That was the end of history. Leave us alone.

That model was vulnerable to rumblings of the misbehaviour of executives and corporations, such as Enron, WorldCom and Ponzi schemes like that of Madoff. But the wheels came off in the 2008 global financial crisis when the selling of mortgages to people who were unlikely to be able to repay them (sub-prime), and their bundling and on-selling as CDOs, was revealed when interest rates turned and the entire banking system was shown to have wholly inadequate asset buffers, leading to the entire system crashing and having to be bailed out by states using taxpayers' funds. Blame was placed at the use of targets, remuneration practices and a constant focus on stock values and reporting driving short-term profits. Short-termism was again held up when it became clear that unconstrained market behaviour on carbon emissions was likely to render all "valuable" assets as irrelevant as the world warmed through human activities.

This is a very short and simplistic account. But it highlights the need for society to take steps to protect itself. So we see changes such as in regulation of activities, corporate governance, concepts of stakeholder value, corporate responsibility, stewardship and so on.

This background provides a warning against complacency and establishing systems that are insufficiently robust. The opportunities for use of data in a new digital and AI world are immense—but they are opportunities for good and bad purposes and outcomes. So we need to think carefully about the design and operation of effective systems that balance prosperity and protection. Those tasks essentially involve employing technical expertise, ethical values and principles, effective governance and transparency, objective scrutiny and opportunities for legal intervention.

Is it inevitable that prosperity and protection are opposing objectives and forces? They need not be. Many sectors achieve successful outcomes and balance. The findings of behavioural and social psychology are underpinning fresh and effective approaches to motivated, effective people in commercial organisations, to basing activities on ethical values, and to engaging so as to increase performance—in outcomes that deliver both economic success and compliant protection. An inspiring example is the global aviation industry that achieves safety through ensuring open and just culture throughout the sector.

We are in the early stages of using and understanding uses of data, some corporate actors are young and huge, many people face difficulties in engaging and complying with new rules, and regulation is new. All of these people and systems will need to evolve. For example, new forms of regulation, engagement and intervention will be required. Protection is not negotiable; it's what society needs, wants and has a right to expect.

I believe that the key concepts in framing the future are: ethical values; cooperation in sharing ideas, information, experiments, learning and making changes; independent oversight; accountability; sharing knowledge, building confidence and increasing trust; and delivering outcomes.

CHRIS HODGES OBE
Professor, University of Oxford

Christopher Hodges is Professor of Justice Systems, and head of the Swiss Re Research Programme on Civil Justice Systems, Centre for Socio-Legal Studies, University of Oxford. He is a Supernumerary Fellow of Wolfson College Oxford.

PROMOTING ACCOUNTABILITY THROUGH REGULATORY LEADERSHIP

By José Alejandro Bermúdez, Former Colombian Superintendent for Data Protection | Partner Bermudez Durana Abogados

Criminal law theorists and academics have argued extensively on when and what to prosecute and the long-term effects of excessive criminalization policies. Should all misdemeanors be prosecuted? Should scarce resources be directed to strengthening cases with a higher societal impact? What is the social impact of obtaining visible results in high profile cases at the expense of choosing selectively?

These questions should probably be considered in enforcement of privacy cases.

In recent decades, we have witnessed an explosion of new privacy regulation, a formidable advance in technology and a correlated increase of enforcement by DPAs, triggered by new business models, advanced analytics and innovative uses of personal data. As a former regulator, tasked with the then new Colombian regulation, we advanced awareness and engaged proactively with stakeholders, but probably could have done things better. In hindsight, the question remains: could we have looked more intensely at the forest instead of focusing on a few trees? Could we have tackled more big problems instead of losing focus with minor violations of the law? Some of the restraints could be blamed on the regulation (many laws mandate regulators to process every single claim), and some were probably a combination of lack of experience, of precedents and of a robust data protection culture.

But even at that initial stage, with a nascent DPA, there was a need to identify the building blocks that would lead to enhanced compliance and to an enforcement that resulted in more protection for individuals - an enforcement that got closer to achieving the results regulators are tasked with. I would argue still that the answer is in a concept now widely deployed in data protection laws and guidelines all across the globe: maintain a focus on accountability.

Since its inception in the 1980 OECD Privacy Guidelines, accountability, a simply worded yet hard to implement principle, has found its way to multiple legislations and guidelines, including the GDPR, LGPD, APEC's Privacy Framework and the Iberoamerican Standards. Practical implementation, however, remains fuzzy, and an important objective of enforcement policy should focus on how to translate accountability provisions into workable practices.

Mandating companies that process data to implement comprehensive privacy management programs (that is, that they materialize the accountability principle through the implementation of effective and demonstrable privacy measures) is the best way of stepping away from a merely compliance approach (where following the law is reduced to ticking boxes in rigid, outdated checklists) towards a model where data protection is embedded in the corporate principles of ethically driven, enthusiastic and responsible organizations.

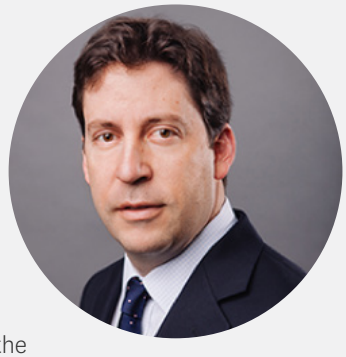
The task for regulators is ever more complicated. New technologies, an unexpected global pandemic, scarce resources and mandates to look into every complaint, to name a few, are hurdles in the way of practical implementation of the law. I strongly believe that a successful and influential DPA should embrace an accountability centered approach, one that privileges organizations which fully commit to the implementation of comprehensive privacy programs, which go above-and-beyond

mere compliance, and which actively engage with their stakeholders and the authorities to work together towards the common goal of protecting the rights of the individuals.

Companies that consciously opt for the hard path, that decide to focus on being transparent, present better choices to individuals, hold true to their promises, commit to drafting in clear language and facilitate the exercise of subject rights, deserve recognition. Some legislations, including Colombia's, have specifically provided that companies who can demonstrate their good practices are rewarded with a favorable approach in enforcement actions. Mistakes can happen, and some situations may result in non-compliance, but the priority should always be in focusing on actions that cause real harm to individuals.

Effective DPAs -- and examples are abundant throughout the world -- devote much of their time and efforts to actively promoting the adoption of accountability-based approaches. They are uniquely suited to act as guiding partners in the interpretation of the law. Their role should then ideally continue to focus on better understanding trends and technologies and generating discussions that lead to better policies and targeted and strategic enforcement. This strategic approach, centered on a continued analysis of the evolving nature of a fundamental right that needs to be balanced with the beneficial uses of data, is a major piece of the puzzle in the search of lawful and responsible uses of data while minimizing risks and avoiding harm and discrimination.

JOSE ALEJANDRO BERMUDEZ
LATAM Advisor, CIPL | Partner, Bermudez Durana Advogados



José Alejandro Bermúdez is Partner at Bermudez Durana Abogados (Colombia). José Alejandro was the inaugural Deputy Superintendent for the Protection of Personal Data in Colombia where he charted a path for Latin American data protection as the promoter of the Colombian Accountability Guidelines published by the Superintendency of Industry and Commerce (SIC). As a member of the Governmental commission appointed to draft the Colombian Data Protection Law and its secondary regulations, José Alejandro helped shape the data protection regulatory landscape in Latin America. He was an ad-hoc observer to APEC's Privacy Subgroup and the OECD Working Party on Information Security and Privacy in the Digital Economy, a member of the Colombian OECD Accession Mission (privacy and digital economy), and served as a member of the Executive Committee of the Ibero-American Network of Data Protection (RIPD). José Alejandro is LatAm Advisor at CIPL and Colombian co-chair of the Latin American Privacy Association.

THE NECESSITY OF INTEROPERABLE DATA PROTECTION REGULATIONS

By Shailendra Fuloria, Chief Information Security Officer, Nagarro

We see technology as a global enabler that makes distance irrelevant and brings people together by bridging the schisms of geographical frontiers and ideologies. Data is fast becoming the fuel to power the engine of technology. In a globalized world, with low barriers on the movement of goods, people, technology and services, access to data will be necessary for innovation leading to societal and economic progress.

Data Protection regulations will be central to establish rights of individuals and create responsibilities for enterprises which need to process data as part of their businesses and setting guidelines to facilitate compliance. It is expected that within the next few years, more than 65% of the world's population would be protected by some data privacy law. Beyond regulatory compliance, we believe that ethical processing of personal data is going to be a critical element in corporate governance. Hence, we must enable trust and accommodate the expectations of individuals in a digital society. This should, however, be done by creating regulations that are interoperable at a global scale. Most organizations (including Indian companies) have a growing global footprint. Regulations that are not globally interoperable would only become business inhibitors and deterrents in the long run. This may also result in making compliance disproportionally expensive, creating significant overheads and overall, challenging to implement. This will be true even for organizations that do not process end-user data (unlike Google and Facebook) but do have subsidiaries and sister organizations across the globe. Interoperable standards would also ensure better security and compliance of data as organizations focus on a uniform technical architecture and compliance framework. This will ensure that personal data is processed and consumed in a responsible way to foster the digital society and economy, without compromising the fundamental rights of individuals – which is the core intent of all data protection regulations.

SHAILENDRA FULORIA
Chief Information Security Officer, Nagarro

Shailendra Fuloria provides leadership to Nagarro's organization-wide information security programs as its Chief Information Security Officer (CISO). Shailendra has previously worked with Eaton, ABB and Cisco in customer-facing and R&D roles related to security. He has been involved in framing several international standards (IEC, NIST) on security for critical infrastructure systems and has chaired several national and international initiatives around security in energy delivery systems. Shailendra is a software engineer by training with a PhD in Information Security from University of Cambridge.

THE COVID19 PANDEMIC AS A DRIVER OF A SINGLE HEALTH DATA SPACE

By Jaanus Pikani, Chairman, ScanBalt & Oliver Stenzel, Director Network Research and Innovation, Novartis

European data space for health data has been developing for several years. However, so far there has been no clear commitment from the European nation states to shape this process in a structured and coordinated way. The national paradigm of subsidiarity in health care is too strong. As a result, the existing European data space is fragmented and exists mainly limited in extent in some member states with more advanced digital ecosystem or around high level innovative centres of science and research. Several examples of evidence on effective data sharing were provided at an international conference of meta-cluster organisation ScanBalt: 30 promising projects for digital solutions in dealing with the COVID-19 crisis were gathered from 15 different European regions. The examples ranged from cross-border data exchange for patient care, decentralised digital patient monitoring or the creation of new databases for research into COVID-19 therapies.

The majority of these initiatives were supported by private-public cooperation. This is certainly the most important lesson from the COVID-19 crisis: A health crisis of pandemic proportions can only be overcome through collaborative efforts between public (academic) and private (industrial) research. The fact that these new forms of cooperation must be digitally designed is now a matter of course that should not even be worth a marginal note - and yet there is still a lack of meaningful digital linkage across national borders in Europe.

Against the backdrop of the COVID-19 pandemic, European scientific and research regions have taken stock of the digitisation of European health systems and formulated a joint declaration, the ScanBalt Declaration "Towards a European Common Dataspace in Health in the Time of COVID-19", describing the current situation, bottlenecks and possible solutions to create a European health data space. The declaration brings together countries known for their innovative digital health systems as well as regions where the pressure of Coronavirus infections has greatly accelerated existing digital care approaches. Input for the declaration comes from countries such as Estonia, Sweden, Denmark, Norway, Finland, Italy, Spain, the Netherlands, Belgium, Portugal, the UK, Austria, Germany and Poland.

As the "voice of European civil society", the participating cluster organisations support the promising digitisation initiatives of the current EU Council Presidency of the countries Germany, Portugal and Slovenia. (see: https://scanbalt.org/eu-health-data-space/)

All initiatives have in common the high importance of data protection - which is indispensable as a basic prerequisite for all activities, whether in care or in research. Data protection is understood here above all as a right of citizens to their data and to self-determined handling of their data. All European citizens must have access to a complete electronic record of their health data and retain control over it in accordance with the EU General Data Protection Regulation. At the same time, European citizens must be free to decide for themselves on sharing their data with for medical treatment, preventive services, research and product development, or for any other purpose they deem appropriate. It is important that they can be confident that potential partners are authorised and permanently vetted. European regulators thus have a key role in building trust in

healthcare institutions. Importantly, the whole thing also only works if the EU agrees on uniform, internationally recognised and tested standards/codes across Europe to ensure interoperability.

To secure this, Europe needs strengthened pan-European institutions. Current promising initiatives from the European Commission include strengthening the European Centre for Disease Prevention and Control (ECDC) to improve its coordination capacity and mandate to respond to the crisis. And at the same time, European policy on the legal situation and legal interpretation in data protection law should be coordinated between the member states on the basis of the EU General Data Protection Regulation in appropriate detail.

But it is not only institutions and health systems that need to be digitised - citizens also need to learn how to handle their health data on their own responsibility. Only informed citizens can make competent decisions about the use and exchange of their sensitive health data. Therefore, we urgently need a Europe-wide support programme to strengthen citizens' digital health literacy.

JAANUS PIKANI
Chairman, ScanBalt

Jaanus Pikani has been practicing surgeon in head and neck oncology, hospital manager of National Cancer Centre and Tartu University Hospitals, secretary general of the Ministry of Social Affairs of Estonia and director the office of the President of Estonia. Currently he is entrepreneur and consultant for the World Bank and chairman of Tartu Biotechnology Park and ScanBalt, a biotech meta-cluster organization of ScanBalt BioRegion.

OLIVER STENZEL
Director Network Research and Innovation, Novartis

Oliver Stenzel is a board member of the meta-cluster ScanBalt MTÜ and head of the digital working group there. As a political scientist, he has many years of experience as a public affairs specialist in various healthcare associations and the German Bundestag. He currently works as Director Network Research and Development at Novartis Germany.

DIGITISATION AND SCRUTINY OF BUSINESS DATA PRACTICES

By Rama Vedashree, CEO, Data Security Council of India

As we scan the landscape of digitization across enterprises, be it Banking, Retail, Travel, Public Services, along with post-pandemic Healthcare and Education too, the platformisation of technology and business has really come centre stage. Every enterprise and public agency, is crafting their digital journey where services are designed harnessing data driven innovation. Services to consumers and citizens are curated and designed from the ground up for smart devices, typically with a cloud-first/native strategy, integrating with a host of ecosystem partners and platforms through APIs and Apps. The volumes of data and velocity of Apps development has seen unprecedented momentum, and post-pandemic, it has only accelerated several notches. The digital economies across the world riding on the internet and cloud platforms have created connected global Data Grids. Companies, Governments, and consumers are contributing to this digitisation but also bringing to fore the many challenges on the state of cybersecurity and privacy in this data driven world.

While every country is pursuing a fast-paced growth trajectory of its economy, riding the digital wave with data as its new currency, Governments and Regulators worldwide are caught in this conundrum or Holy Grail of making businesses balance privacy and user trust with data driven business growth. Consumer trust and regulatory scrutiny are the two major challenges that businesses worldwide transitioning to a Digital and a Data Enterprise must grapple with. They must also demonstrate increased accountability and transparency with their data practices.

CEOs and Boards of technology-led enterprises are now beginning to give attention not just to Cyber Risk but some Governance and Policy dimensions around Data. This leadership attention to company's Data Strategy and sustainable growth is not driven just by evolving Global Regulations but also in equal measure to position themselves as a trustworthy data fiduciary in the eyes of its users and consumers. It's only a question of time before every "Corner Office" or Board Room, even if in the short term, over their virtual calls, discussions with their teams, delve into:

- Rapidly evolving regulations and laws around data protection and privacy and company's readiness to conform in every geography they operate in.
- Is the company being transparent and accountable of their data practices and AI-based innovation strategy and are they being responsible enough in their data-centric innovation for their new products and services?
- Is Inclusion and Fairness driving the company's data practises and ensuring algorithms are not comprising the company's business ethics and values both with consumers and employees?
- Is the company ready for a paradigm shift in accepting the consumer as a key stakeholder and enabling a user-first approach to their products design and privacy practices?

- With new expectations from governments and communities to democratise and open up data for larger public and social good, is the company crafting a data strategy that can meet these new demands without diluting its market positioning and profitability?

- Does the company fully comprehend ramifications of balancing privacy and user trust with National Security and Lawful access requests for Crime Investigation?

- With global discourse around Data Monopolies and Competition and regulatory scrutiny on Big Tech, will there be an impact on company's ecosystem partnerships and going global?

- Is the company crafting a focus on ecosystems collaborations and partnerships with start-ups to harness the real power of data centric innovation?

- Is the Company doing enough in educating employees and users about being Privacy-Aware and staying safe online?

In the short term, while there is a lot of public discourse and a worrying regulatory and civil society scrutiny around Business's data practices, I remain positive that every Technology-ed Business will make users and their expectations of Privacy central to their Digital strategy. There are already many enterprises leading the way in making Privacy and consumer trust as a foundational pillar of their digital business and the benchmarks they are setting, will ensure that their peers and even competitors take a cue.

RAMA VEDASHREE
Chief Executive Officer, Data Security Council of India

Rama Vedashree was previously Vice President, NASSCOM leading all initiatives in Domestic IT, eGovernance and Smart Cities among others. At NASSCOM, she has also led the Healthcare initiative in partnership with apex Health Sector body, NATHEALTH. She is also anchoring a new initiative of the industry on making India a global hub for cyber security. With a rich and varied experience of 28 years in the industry, she has had long stints at NIIT Technologies, Microsoft and General Electric.

THE NEW HEALTH DATA AND PRIVACY ECOSYSTEM: WHAT ARE THE GOVERNANCE IMPLICATIONS OF REAL-TIME HEALTH DATA ECOSYSTEMS?

By Pam Dixon, Founder & Executive Director, World Privacy Forum

Health data ecosystems have experienced radical changes over the course of the pandemic. Among the most striking of the changes is an accelerated shift of retrospective health data systems to real-time or near real-time systems, some of which are also predictive. These changes signal a new level of health data ecosystem maturation, and while the changes should not be avoided, they do create meaningful implications for data governance and privacy.

Prior to the pandemic, real-time health data ecosystems have not been a fully achieved norm due to considerable investment and infrastructure requirements and costs. In the financial sector, where real-time systems are well-established out of necessity, FINRA is a standout exemplar, with a high-capacity, real-time data ecosystem that facilitates real-time compliance and auditing.[1] The Andhra Pradesh Real Time Governance Center, another early exemplar, built its system in part by utilizing existing Aadhaar infrastructure. The RTGC core dashboard tracks mobile medical units in real time, as well as hospital bed capacity data, among other data.[2]

Now, having experienced a global health crisis that has provided abundant necessity for real-time health sector information, a more expansive shift to real-time health data systems is underway. Numerous new systems have been established relating to the pandemic. A collaborative group of UK universities have already developed a "near real-time" UK-wide notification system in partnership with the British Paediatric Neurology Association (BPNA). The system identifies neurological symptoms associated with COVID-19 in children. The data has yielded results; the Lancet published a study based on the data that documented the extent of brain complications of COVID-19 in hospitalized children, and the BPNA published critically important new guidance based on the data.[3] More systems are on the way or in rapid development, including those addressing the pandemic and other health topics.[4]

Going forward, the US and other governments are keen to construct the data infrastructures of tomorrow, which many health sector stakeholders describe as real-time and bidirectional.[5] The health care sector has a roadmap to modernize its data infrastructure. A similar roadmap for modernizing data governance in tune with the new infrastructures is largely absent, however. It is reasonable to prepare now for the data governance and privacy implications that real-time ecosystems create.

1 *FINRA, https://www.finra.org/#/.*

2 *Andhra Pradesh Real Time Governance Center, Core Dashboard, https://core.ap.gov.in/CMDashBoard/Index.aspx. See in particular the Health and Family Welfare tab: https://core.ap.gov.in/CMDashBoard/UserInterface/HealthFamilyWelfare/HealthFamilyWelfareReport.aspx.*

3 *COVID-19 and Paediatric Neurology, 31 March 2021. BPNA. https://bpna.org.uk/_common/show_unpro_doc.php?doc=20210331GUIDANCECovid19andPaediatricNeurology_117c9ae67575bb19dbab1b208f89c64b.pdf. See also Ansel Hoang, Keven Chorath et al, COVID-19 in 7780 pediatric patients: A systematic review. The Lancet, June 26, 2020. https://www.thelancet.com/journals/eclinm/article/PIIS2589-5370(20)30177-2/fulltext.*

4 *See for example The Health Improvement Network (THIN), a proprietary primary care database which is considered to be one of Europe's largest health databases. THIN facilitates real-time analysis of response to treatments. https://www.cegedim-health-data.com/cegedim-health-data/thin-the-health-improvement-network/.*

5 *Data modernization initiative, Centers for Disease Control and Prevention, https://www.cdc.gov/surveillance/surveillance-data-strategies/data-IT-transformation.html. See in particular CDC Data Modernization Roadmap: https://www.cdc.gov/surveillance/pdfs/318212-A_DMI_LogicModel_July23b-508.pdf.*

Issues to consider include:

Automating governance: Data formatting and tagging is essential in real-time data ecosystems. GDPR requirements for technological proof of compliance provided an early glimpse into baseline work that will need to go into data systems that operate in real-time. Further aspects of governance that go beyond proof of compliance will need to be coded in to such systems.

Role of standards: Standards in the health sector, such as HL7 and the FHIR standards, and the standards development organizations that support this work, occupy extremely important roles in real-time systems. Real-time health data exchange, transformation and analysis depends on these standards. HL7 and FHIR already exist, but more standards will need to be developed, with governance and privacy stakeholders involved.[6]

Role of human oversight (and more standards): When data moves and is analyzed at real-time speed, older governance models may not be effective. What is missing in real-time health data systems are freshly tooled administrative and procedural standards for governing health data, inclusive of legal and ethical protections. Here, FINRA's implementation model can provide assistance as a template for real-time governance and privacy.

Accuracy: In real-time data sets and analysis, will there be new, better standards for determining data accuracy? If data is being utilized at speed, the data must be dependable for those utilizing it and those being impacted by it. The shift to real-time data systems is an important opportunity to improve accuracy requirements and levels.

Redress and correction: Redress and correction procedures need to be built into real-time systems from the beginning. At speed, systems will need to be coded for privacy; for large health ecosystems analyzing billions of data events per day, human review is insufficient. There is an opportunity here to build real-time correction, and real-time redress models.

Health data ecosystems are in a state of significant flux and adaptation to a new health reality influenced by the global pandemic. As data systems operating in real-time and bi-directionally increase in number, size, and complexity, pressures resulting from the implications for health data governance and privacy also increase. There are new risks to understand and mitigate, and there are new possibilities for making improvements. It is important for all stakeholders to work cooperatively to address both the risks and the opportunities that real time health ecosystems bring.

PAM DIXON
Founder & Executive Director, World Privacy Forum

Pam Dixon is the founder and executive director of the World Privacy Forum, a respected public interest research group. An author and researcher, she has written influential studies in the area of privacy in the area of identity, AI, health, and complex data ecosystems and their governance. Dixon has worked extensively on privacy across multiple jurisdictions, including the US, India, Africa, Asia, the EU, and additional jurisdictions. Dixon currently serves as the co-chair of the Data for Development Workgroup at the Center for Global Development (CGD). The working group is researching the impact of Covid-19 on low and middle Income countries. She also serves as a delegate for OECD, most recently on the AI Experts Group, among other multilateral work in the area of data governance. Dixon is a co-chair for a UN Statistics Division workgroup where she is focused on complex data governance systems. Dixon has been presented her work on complex data ecosystems and data governance to the National Academies of Science and the Royal Academies of Science, most recently in 2020. She served on the HL7 board, and contributed to that standard.

6 *FHIR, Fast Healthcare Interoperability Resources, is a foundational interoperability standard. http://www.fhir.org.*

A FRESH START FOR DATA PROTECTION

By Richard Thomas CBE, Former UK Information Commissioner | Global Strategy Advisor, CIPL

What would data protection look like if we started with a blank sheet of paper? This is a fantasy. It will never happen. Even the dream gets clouded by what already exists. But dreams are healthy and sometimes gives valuable insights.

Let's start with the basics. The New General Data Protection Law (NGDPL) must be **short, clear and simple**. It must not be incomprehensible to the general public, let alone the organisations (small and large) which are supposed to observe its requirements. There must be something wrong when a law needs 173 Recitals and 99 Articles and still gives rise to uncertainty or confusion, even amongst its regulatory bodies. It should be written in **Plain Language** and require all information provided to data subjects to be in Plain Language. And my fantasy gets rid of the jargon. Certainly no more "data subjects" - meaningless and subjugating to most people. Let's stick to men, women, children, consumers and citizens.

And let's aim to keep the paperwork (or digital communications) to the absolute minimum. Transparency is fundamental, but bombarding people with gobbledegook privacy policies serves little purpose, especially where the small print effectively obscures dubious activities. Worse still, creating a complete world of liars who confirm they have read and understood the garbage. The "notice and consent" approach to data protection should long since have been dead and buried.

To be less prescriptive and less process-based, NGDPL must be crystal clear with its **Objectives**. It must set out what it intends to achieve. Better still, it should state what it seeks to avoid. Good laws prevent evil, rather than promote virtue. This largely means that the new Law should be based on **Harms from the misuse of personal information**. This is a great deal more concrete than abstract references to fundamental rights and freedoms which prove actually not to be fundamental at all.

What harms? Any unlawful, unfair or deceptive use of personal information should be outlawed. So too should any sharing or use which breaches confidentiality or exceeds the person's reasonable expectations. Beyond that, the risk-based approach provides most of the answers. Inaccurate, out-dated or wrongly-obtained personal information which leads to **tangible harm** - whether physical or economic – should clearly be prohibited. This includes bodily harm, loss of liberty or freedom of movement and financial loss. **Intangible harm** covers such matters as reputational damage, personal, family or social detriment, chilled freedom of speech and other unacceptable intrusions into private life. **Societal harm** which damages democratic values must also be covered, for example excessive state or police power and loss of social trust.

The important point about a harms-based approach is that it will send clear signals to everyone about what the Law is aiming to achieve. It also shifts attention to **outcomes**. Organisations should stop things going wrong or harms occurring – unacceptable outcomes - and be held accountable if they fail. This is better than lots of detailed procedures (e.g. on international transfers) which are driven by what might go wrong. Accountability for outcomes is better than accountability for "demonstrating compliance" with largely procedural requirements.

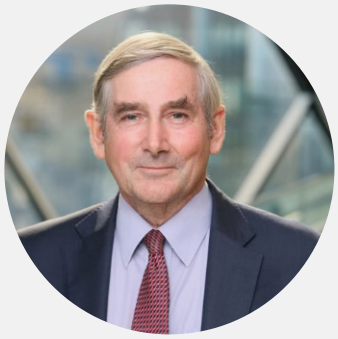
NGDPL will of course recognise that the digital world is global and so have **worldwide application**, or at least cover all liberal democracies. (I repeat this is a fantasy.) It will especially target **governmentally-held data** (including police and security

forces). This recognises that governments have wide mandatory powers to obtain data, hold much more than commercial bodies, are not restrained by competitive pressures and can cause much greater harm when things go wrong.

The top priority for **Supervisory Authorities** should be to help organisations to "get it right". The new Law needs to give them strong enforcement powers, but expect these to be concentrated on deliberate, high-risk or repeated non-compliance with the Law or situations where substantial harm actually has resulted. And all complaints should be diverted to Ombudsmen or similar institutions, rather than distracting from normal regulatory functions.

The blank sheet of paper does not exist. NGDPL will never be enacted. Perhaps a dream may be a nightmare for others. Or, perhaps a fantasy could at least be a starting-point for simplifying existing laws.

RICHARD THOMAS CBE
Former UK Information Commissioner
Global Strategy Advisor, CIPL



Richard serves as Global Strategy Advisor to the Centre for Information Policy Leadership (CIPL) at Hunton Andrews Kurth LLP, a path-finding global privacy and security think tank. He brings to the position nearly 40 years of experience working across the private and public sectors.

Prior to joining CIPL, Richard was appointed by HM Queen to serve as Information Commissioner for the United Kingdom from November 2002 to June 2009. In this position, he held independent status and reported directly to Parliament. While at the Information Commissioner's Office (ICO), Richard had a wide range of responsibilities including regulatory powers under the Freedom of Information Act of 2000, the Data Protection Act of 1998 and related laws.

In 2008, Richard was recognized as "Privacy Leader of the Year" by the International Association of Privacy Professionals (IAPP) and ranked third in Silicon.com's global "IT Agenda Setters" poll. That year, he also served as a visiting professor at Northumbria University.

Richard is frequently sought as a keynote speaker for industry conference and events and is regularly quoted in the business and trade media.

WE NEED A BRETTON WOODS FOR DATA

By Elizabeth Denham CBE, Consultant, Baker & McKenzie LLP and former UK Information Commissioner

In July 1944, the world was still at war. Allied forces fought to liberate France. Battles in the Pacific would continue for another year.

In New Hampshire, USA, the mood was a little different. There, economists and politicians gathered to deliberate how the world could rebuild after the war.

Within weeks, international delegates made a series of agreements that continue to influence our world today, notably via the International Monetary Fund and World Bank. Those delegates appreciated the challenges that individual states faced in rebuilding their own nations, which required international solutions.

Today's challenges may not compare with that terrible, turbulent time. But international cooperation remains critical to progress. Our digital world is borderless, but its checks and balances are domestic — that brings problems. It means that our systems for managing international data flows are based on assessments of how other nations' laws measure up to our own, no matter how many flaws we may be willing to acknowledge in our own systems.

Some ongoing work mitigates such problems. Under Japan's leadership, the G20 adopted "data flows with trust" as the theme of its 2019 meeting. In 2021 the G7, under the UK Presidency, convened policy discussions about responsible use of data. The Global Privacy Assembly (data protection commissioners around the world) has undertaken ambitious activities for international collaboration. The Organisation for Economic Co-operation and Development (OECD) continues to draft governance standards for intelligence services. And in April 2022, the US, Canada, Japan, and Singapore announced a global certification system based on the Asia-Pacific Economic Cooperation's (APEC) Cross-Border Privacy Rules. But all of this work only takes us so far. More ambitious approaches are urgently needed.

Adequacy assessments are quickly proliferating in national laws, and the number of data localization measures has more than doubled in the past four years. Considering whether another nation's laws offer the same protections as your own is a difficult process, and it can too often result in highly limiting yes-or-no decisions. Throw geopolitics into the mix, and adequacy assessments can become impossibly complex. Where agreements appear vulnerable to court challenges, they fail to offer the surety that businesses crave.

History teaches that domestic solutions cannot solve international problems. And that idea returns us to Bretton Woods. In 1944, The Bretton Woods conference was attended by 730 delegates from 50 nations. They were united in one understanding: that the old systems had failed, and a new one, based on international cooperation, was needed. The Bretton Woods system of monetary management established the rules for commercial and financial relations among the US, Canada, Western Europe, Australia, and Japan. We need similar agreements to consistently and responsibly manage data, which is inherently borderless and integral to digital innovation. Data flows rely on public trust that can only be earned through sensible and comprehensible protections.

We do not need one data law for all nations to follow. Instead, we need globally applicable standards for how to transfer and manage data with trust. Such standards would allow different legal systems to work in tandem. Membership within an international data accord would require countries to demonstrate their commitment to data protection and independent enforcement. Crucially, the bar for membership should be lower than adequacy. We should not necessarily ask countries to demonstrate that their laws offer the same safeguards as those outlined in the General Data Protection Regulation, for instance. Bringing as many countries as possible into the fold is desirable; we want to provide surety to the many rather than the few. Further, businesses would benefit from operating under a broad system of requirements rather than according to the stipulations of partnerships formed with individual nations. Ideally, people should understand basic protections that limit uses of their data, wherever it may travel around the globe.

Who could possibly convene the necessary discussions to create such a system? The UN? The OECD? The Council of Europe? The World Trade Organization? We know that the political will to build an open, rules-based, and international regulation is growing. We cannot build an innovative digital economy without collaborating on constructive alternatives to the current situation. We need 21st-century thinking to address 21st-century problems.

ELIZABETH DENHAM CBE
Consultant, Baker & McKenzie LLP and former UK Information Commissioner

Elizabeth Denham CBE brings extensive international regulatory expertise to her portfolio career. She served as the UK Information Commissioner from 2016-2021, following a decade of roles as a data protection and information rights regulator in Canada. As Information Commissioner for the UK, she built and led the largest data protection regulator in the world and Chaired the Global Privacy Assembly (international forum of data protection commissioners) from 2018-2021.

Elizabeth is committed to making digital technologies and data work for the benefit of society. Under her leadership, the ICO embarked on some of the most daunting cross-border investigations on the misuse of individuals' data -- including her investigation into political micro-targeting and election interference, data brokers and credit reporting agencies, and use of facial recognition technology by commercial firms and the police. She is passionate about the ethical and safe collection, storage and use of data. A highlight of her time at the ICO was drafting the first 'privacy by design' statutory Children's Code – a set of fifteen enforceable standards to protect children's safety and agency on- line. This Code is having global impact as technology companies and services making meaningful changes to their services to comply with the rigorous standards in the UK Code.

In the 2019 New Year's Honours list Elizabeth was awarded a CBE for her services to protecting people's privacy. In 2020 she received the BCS Society Medal, which recognises an outstanding individual whose work and values have helped to enhance the reputation of digital technology and its contribution to improving our lives. In 2021 she received an honorary doctorate from the University of Victoria for international leadership in information rights.

She serves on the board of 5Rights, a Children's online rights foundation, and works as an international advisor to Baker McKenzie's data and tech practice.

HARNESSING COMPETITION TO ENSURE EFFECTIVE DATA PRIVACY: PRACTICAL AND PROCEDURAL CONSIDERATIONS

By Orla Lynskey, Associate Professor, London School of Economics (LSE)

The digital services landscape is dominated by a handful of firms whose decisions and operations have an outsized impact on whether we can enjoy our fundamental rights and the extent to which we may do so. Market concentration is therefore no longer a potential economic issue, but has now become of broader societal relevance. This is recognized in the EU through the asymmetric approach taken to recent digital regulation: the Digital Services Act imposes specific additional requirements on "VLOPs" (Very Large Online Platforms), while the Digital Markets Act (DMA) applies to entities that act as "gatekeepers" for core platform services. The latter Act explicitly connects with EU data protection law in numerous ways. For instance, the DMA definitions of key terms such as consent, profiling and personal data are those found in the EU General Data Protection Regulation.

These EU examples of asymmetric regulation remain the exception. Typically, it will be for competition and antitrust enforcement agencies to assess whether market practices, including mergers and acquisitions implicating personal data processing, impede competition by leading to privacy deteriorations. It is now widely recognized that the consumer welfare standard used to assess competitive practices can incorporate data protection considerations as an issue of product or service quality. Indeed, we have moved from a period when connections between data protection and competition were discussed hypothetically to one where this connection is having tangible impact. Antitrust complaints against Apple concerning its introduction of App Tracking Transparency provide a fascinating example.

Major matters of substance still require further attention. Most notably, it remains unclear whether competition authorities will recognize that the actions of individual consumers can negatively impact the privacy of consumers as a group. Yet, it is now high time to consider the procedural and practical dimensions of the involvement of competition regulators in data protection matters. In particular, how can we ensure that digital rights advocates can harness competition law to render digital rights more effective? Civil Society Organization (CSO) Privacy International has recently published a report on this topic. What emerges is a mixed picture: competition authorities and CSOs in the Americas and Europe are already addressing data and competition issues whereas this is not yet the case in Africa or Asia. Importantly, the report notes that effective competitive assessment is closely linked to the existence of a data protection framework, which provides tools to assess anti-competitive behavior and acts as a source of remedies and interventions.

It is clear from this report that competition authorities particularly value the expert opinion of CSOs. Yet, beyond resourcing issues, CSOs also encounter difficulties in establishing standing. In the EU, for instance, the European Commission's investigations of anti-competitive agreements and abuses of dominance are not adversarial proceedings. A CSO can strengthen its position in these proceedings by lodging a complaint; however, it must show that its economic interests have been harmed. It will be essential in the EU and elsewhere that rules are interpreted in a way that reflects the broader acceptance that privacy forms part of a product's and service's quality. Where CSOs have been given the opportunity to participate – for instance, Privacy International's and the European Consumer Organisation's (BEUC) involvement in the Google/FitBit merger investigation – their

involvement has been impactful. This is a brave new world for CSOs, competition agencies and data protection authorities. Successful engagement may secure the holistic and effective enforcement of data protection law called for by the European Data Protection Supervisor in 2014, while a failure to facilitate these interactions will lead to enforcement inefficiencies and artificial regulatory silos.

ORLA LYNSKEY
Associate Professor, London School of Economics (LSE)

Dr. Orla Lynskey is an Associate Professor at the LSE Law School and a Visiting Professor at the College of Europe, Bruges. She is an Editor of International Data Privacy Law and writes and speaks on data protection, privacy and technology regulation.