Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Data Protection & Privacy

Contributing Editor
Alan Charles Raul
Sidley Austin LLP

chambers.com

2020

INTRODUCTION

Contributed by: *Alan Charles Raul,* ***Sidley Austin LLP***

Digital Governance: Regulating Privacy and Data Protection for Emerging Technologies

Citizens, consumers and companies could use more guidance than they're currently getting on the governance and accountability principles appropriate to managing personal and sensitive data, and the deployment of human-centric digital technologies. The world's regulation of privacy and data protection as well as enforcement related to disinformation, micro-targeting and other profiling, behavioural and location tracking, artificial intelligence, facial recognition technology and the collection of data from ubiquitous sensors and connected devices is evolving with insufficient analysis and co-ordination. Emotion and presumption appear to be dictating too much policy development in state after state and country after country. More attention must be focused on how emerging technologies actually hurt people and critical societal functions – and how to abate those harms – while honestly addressing and balancing the trade-offs.

Given that the USA has not yet enacted comprehensive federal legislation, maybe the time is right for it to start leading with a fresh set of insights. Congress could do this immediately by adopting legislation that would establish a Digital Accountability and Privacy Co-ordinator in the Executive Office of the President and empowering that official to develop information technology policy in the White House and federal agencies. The new Co-ordinator should also be authorised to convene state and international regulatory bodies in the interests of advancing, rationalising and harmonising the world's approach to regulating the least territorial commodity in the history of the globe – data.

If we do not create a clear consensus on governing principles soon, other nations that may not equally share our values – if not machines themselves – will certainly do it for us before too long. A few thoughts are offered below on the relevant principles for digital policy development and co-ordination.

Policymakers ought to spend more time defining what "data" risks warrant government regulation and considering whether and how cost-benefit analysis should be applied to a fundamental right like privacy. Rigorous analysis is especially crucial when intangible data-related or digital harms are at stake. Systematically characterising the harms that warrant prevention, abatement, deterrence and punishment comprises and defines the "benefits" of privacy and digital regulation. The "costs" of such regulation are embodied in the price of trading off other societal interests if data and digital technology are either "over-regulated" or enforcement resources are misdirected toward illusory, rather than real, risks.

The right balance can be achieved by identifying the actual harms and risks of abusive data practices that warrant prohibition or restriction. Examples of concrete harms would obviously include identity theft; significant reputational embarrassment; revelation of sensitive private facts; bias and discrimination; lost economic opportunity; adversely affected significant interests like legal outcomes and sentencing, housing, insurance, etc.

Less obvious but nonetheless real risks would include manipulation of thought through micro-targeting and false information and loss of human agency or opportunity through profiling and micro-targeting; automated decision-making; or technologies relying on AI, facial recognition, predictive profiling, social scoring, etc.

On the other hand, the relevant trade-offs and costs of potential over-regulation that society needs to consider include handicapping the ability of governments to protect their citizens' personal safety and physical security; encroachments on freedom of speech and the right to receive information; impaired technological innovation; limits on economic growth; constrained organisational flexibility; diminished consumer choice; reduced personal convenience; etc.

Given the universal acknowledgement among Western democracies that privacy is a fundamental human right, it bears emphasis that there is both a legal obligation and a practical necessity to balance privacy and data protection against other fundamental rights and important interests of society. The European Union's principle of proportionality is essentially the embodiment of this "balance."

Lest there be any doubt about the necessity to balance the fundamental human rights of privacy and data protection against other considerations, the legal authorities excerpted below should remove it:

Recital (4) of the EU's 2016 General Data Protection Regulation (GDPR), states:

"The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data,

freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

In applying GDPR in Google v CNIL (September 2019) (Right to Be Forgotten), the CJEU stated:

"The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.... in particular the respect for private and family life, … the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information [and] freedom to conduct a business … The balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of internet users, on the other, is likely to vary significantly around the world."

In establishing and reorganising the Privacy and Civil Liberties Oversight Board (PCLOB) in 2004 and 2007, the US Congress stated (in 42 USC 2000ee) that:

"in conducting the war on terrorism, the Government may need additional powers and may need to enhance the use of its existing powers [and] This shift of power and authority to the Government calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life and to ensure that the … choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend. … [And thus the purpose of PCLOB is to] analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such [national security] actions is balanced with the need to protect privacy and civil liberties…"

Under the Federal Trade Commission Act, including with respect to privacy protections for consumers, in 1994, Congress required the FTC to apply cost-benefit analysis before prohibiting business practices as "unfair" (in 15 USC 45(n)):

"The Commission shall have no authority … to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. …"

In providing flexibility and protections for online platforms in 1996, Congress stated its policy to minimise government regulation of the internet to promote economic growth and innovation (in 47 USC 230):

"The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens. … The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation… Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services… It is the policy of the United States—… to promote the continued development of the Internet and other interactive computer services and other interactive media;… to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation…"

In addressing the use of personal data for political campaigns in March 2019, the European Data Protection Board stated:

"Engaging with voters is inherent to the democratic process. It allows the preparation of political programmes, enables citizens to influence politics and the development of campaigns in line with citizens expectations. Political parties, political coalitions and candidates increasingly rely on personal data and sophisticated profiling techniques to monitor and target voters and opinion leaders. In practice, individuals receive highly personalised messages and information, especially on social media platforms, on the basis of personal interests, lifestyle habits and values. Predictive tools are used to classify or profile people's personality traits, characteristics, mood and other points of leverage to a large extent, allowing assumptions to be made about deep personality traits, including political views and other special categories of data. The extension of such data processing techniques to political purposes poses serious risks, not only to the rights to privacy and to data protection, but also to trust in the integrity of the democratic process. The Cambridge Analytica revelations illustrated how a potential infringement of the right to protection of personal data could affect other fundamental rights, such as freedom of expression and freedom to hold opinions and the possibility to think freely without manipulation."

***

Accordingly, thoughtful digital policymakers should consider the following factors.

Contributed by: *Alan Charles Raul,* ***Sidley Austin LLP***

- Acknowledging that privacy is a fundamental right is not tantamount to concluding it is an absolute right; privacy and data protection rights must be proportionate and balanced against freedom of expression, the right to receive information, freedom to conduct a business, and other fundamental rights.
- Granting privacy rights to restore and support individuals' rights to informational autonomy is not the same as, and does not require, granting economic rights to data generated through another entity's investment, sweat equity and proprietary processes; moreover, treating personal information as though it were owned by its data subjects could inhibit productive derivative uses of data, and slow down machine learning, development of AI, and big data applications that could lead to new cures, etc.
- Banning facial recognition technology to protect against bias could interfere with effective law enforcement and private sector security, and diminish consumer convenience.
- Restricting corporate use of personal data impacts commercial speech and may limit consumers' access to – and could impair society's interest in – innovation, convenience, consumer choice and lower prices.
- Protecting data through encryption, and other heightened barriers to government access to personal information (through appropriate due process safeguards), can lead to less effective law enforcement and weaker protection against terrorism or national security threats.
- Imposing strict controls for content moderation would result in less online disinformation, terrorist propaganda, and hate speech but would run counter to the dictates of the First Amendment and the incentive structure that has allowed the internet to flourish under Section 230 of the Communications Decency Act (which unleashed digital platforms by liberating them from full liability for the content generated by their users).
- Allowing microtargeting based on personal information, online behaviour and browsing data, AI, geolocation tracking technology, and facial recognition could yield more relevant advertising and greater convenience, but could also result in more political manipulation, biased commercial outcomes, social scoring, greater pre-determination of preferences and choices, and ultimately, perhaps, more government surveillance and control.
- Imposing a "precautionary principle" for data protection could lead to over-regulation compared to the relative freedoms of "permission-less" innovation and deployment.
- Regulating privacy and data protection pursuant to cost-benefit analysis requires effective valuation of critical interests in human dignity, autonomy and agency.

***

All in all, regulating privacy, data protection and digital technology is considerably more complex than one would gather from present legislation and regulation. We can hope, however, that enlightened new leadership somewhere in the world will help lead to more meaningful and protective digital policy soon.

INTRODUCTION

Contributed by: *Alan Charles Raul,* ***Sidley Austin LLP***

Sidley Austin LLP is a global law firm with 2,000 lawyers in 20 offices around the world. The firm's privacy and cybersecurity group has more than 70 professionals across offices in the USA, London, Brussels, Hong Kong, Singapore and Tokyo. Sidley Austin represents clients in a broad range of sectors, including financial services, life sciences and healthcare, communications and media, information service providers, professional services and internet companies. The firm undertakes highly sophisticated legal counselling and advocacy, and provides actionable legal advice on challenging and novel questions of privacy and information law. Sidley's lawyers focus on privacy, data protection, information security, internet and computer law, e-commerce, consumer protection, outsourcing, competitive intelligence and trade secrets, information management and records retention, and responding to cybercrimes and network intrusions. The team also handles litigation and government investigations; crisis management and incident response; compliance and regulatory counselling on all data protection laws, such as GDPR and CCPA; legislative and policy developments; and international data transfers.

Contributing Editor

Alan Charles Raul is a partner and the founder and leader of Sidley's privacy and cybersecurity practice. He represents companies on federal, state and international privacy, cybersecurity and digital technology issues. His practice covers global data protection and compliance programmes, data breaches, crisis management, consumer protection issues and internet law. Alan advises companies on cybersecurity preparedness and digital governance, and on litigation, regulatory defence, internal investigations, and policy advocacy. He handles consumer class actions, enforcement matters and public policy involving the FTC, State Attorneys General, the SEC, the FCC, the DOJ, international data protection authorities and other government agencies. Alan is a member of the American Bar Association's Cybersecurity Legal Task Force, the Technology Litigation Advisory Committee of the US Chamber Litigation Center, the PLI's Privacy Law Advisors Group, the governing Board of Directors of the Future of Privacy Forum, and the Center for Democracy and Technology's Advisory Committee.

Sidley Austin LLP

1501 K Street, N.W.
Washington, DC 20005

Tel: +1 202 736 8477
Email: araul@sidley.com
Web: www.sidley.com

SIDLEY