Privacy in the age of data: Regulation for human rights and for the economy

> ***Organisations must design products for privacy and with privacy in mind***
>
> **Jules Polonetsky**, CEO, Future of Privacy Forum

Just about every day we learn about a new use of data that has the potential to enhance efficiency and improve our quality of life. Healthcare, transport, environmental protection, education, city services, entertainment and other areas are being revolutionised by the development of new technologies that use data to make smarter decisions.

In sector after sector new uses of data provide great value to individuals, organisations and society at large. Location information is used to improve traffic flows, reduce waiting times in shops, help the blind navigate airports and provide drivers with essential real-time navigation information. Wearable devices give us granular information about ourselves beyond what anyone could have imagined just a few years ago, helping us make informed decisions about our eating, sleep and exercise habits. The rapid spread of low-cost sensors is transforming everything from living rooms to workplaces to entire cities, helping them to become 'smart' environments.

Scientists use data collected by search engines to find cures for diseases or to identify harmful drug interactions. Financial providers perfect algorithms that identify suspicious account activity, helping prevent fraud and protect our

accounts. Content providers tailor their offerings to our tastes, serving us with the movies, TV shows, music, books and articles that we like.

Governments provide services seamlessly, cutting nerve-wrecking wait times and simplifying bureaucracies to better serve populations, including elderly people or individuals living in remote places. In the near future autonomous vehicles will roam our streets, minimising road casualties and streamlining traffic in busy urban arteries and highways. Drones will deliver products straight to our door.

These new technologies and business models, ranging from big data and artificial intelligence to the 'internet of things', use data as a critical input. Often the data is personal, including sensitive or intimate details about individuals' behaviour, personality traits, preferences, demography, social networks, health, financial situation and even genetics.

As one former European consumer protection commissioner put it, personal information has become not just "the new oil of the economy" but also "a new currency for the digital age". But much like the use of oil or currency requires rules and regulations, so too does the data economy. It needs an ethical and legal framework to prevent excess and ensure responsible use of individuals' information.

The explosion of data triggers privacy issues that governments and responsible businesses need to confront head-on. The same technologies that are used to market, entertain, transport and educate can be misused for discrimination, profiling, stigmatising and targeting based on sensitive criteria that can risk embarrassment and exposure as well as financial or even physical harm.

Born in an age of mainframe computers, before the advent of the commercial internet, not to mention mobile, cloud and the internet of things, the long-standing Fair Information Practice Principles, which for decades have governed how organisations around the world handle personal information, are increasingly strained. Principles that focus on minimising data collection and specifying in each case exactly how information will be used are challenged by a world awash in data. More problematic, providing individuals with transparency and seeking their consent for data collection and use has largely evolved into a practice of drafting endless privacy notices that no one reads or understands, and presenting consumers with rote tick boxes that are viewed as a nuisance (and are ignored).

In a world of drones, smart lighting, and embedded medical devices, the goals of traditional privacy regulations remain true, but the means of execution need to be updated. This can include interactive privacy tools and dashboards, and more generally recognition that beyond legal compliance, organisations must design products for privacy and with privacy in mind.

The United States and Europe are often viewed as having different approaches to data privacy. European data protection laws view privacy as a fundamental human right.

Consequently, in Europe companies cannot process personal data without a clear reason, such as consent or a legal obligation. In the US, where privacy is primarily considered part of consumer protection, the default is different; organisations can use data unless doing so would be deceptive or unfair, or if there is a restrictive sector-specific regulation.

Fortunately for individuals in the US, a plethora of federal and state rules, many of them similar to European data protection regulations, govern the use of sensitive data in sectors such as healthcare, financial, credit reporting and insurance, as well as data about employees and children, and biometric and genetic information. Moreover, anti-discrimination laws in employment, housing, credit and insurance prevent abuse of data to discriminate by race, age, religion, gender and other protected categories. State laws increasingly go further, with emerging provisions addressing innovations in facial recognition, drones, education technologies, biometrics and more. But at a fundamental level, the US and EU privacy frameworks are alike. The two major allies and trading partners share a deep-seated recognition of the importance of privacy as a fundamental normative, social and ethical value, and seek to protect individuals' privacy from governments and businesses in various ways.

One of the major policy developments in the personal data space is the arrival of the European General Data Protection Regulation, which will come into force in May 2018. While born in Europe, the GDPR reaches well beyond European borders, applying to companies all over the world that target their services at consumers in Europe. The new law builds on the 1995 Data Protection Directive and on member state legislation, intending to harmonise the framework across Europe. The GDPR introduces new individual rights, such as the right to be forgotten and data portability, and empowers regulators with significant penalties, which will grab the attention of corporate boards.

Will the new law create an uneven playing-field, where companies that collect massive amounts of data to train algorithms and develop a new generation of services powered by artificial intelligence establish well-staffed and budgeted compliance departments, while newer more nimble players feel stifled by regulatory risk? Or will the law create an environment of trust that nurtures European innovation and supports a techno-entrepreneurial surge?

Furthermore, while much of the global policy discussion has focused on the EU and US, technological innovation is surging in other parts of the world. For example, China-based e-commerce company Alibaba has experienced explosive growth, with its CEO predicting the adoption of artificial intelligence, big data and cloud computing that would revolutionise online retail. Will technological advances that rely on access to data shift to countries where access to data is easier and where privacy regulation is nascent?

To a great degree, the answers to these questions depend on the ability of European regulators to provide certainty with regard to the

interpretation and application of the new law, as well as its companion e-privacy regulation, which, when finalised, will govern some of the same data covered by the GDPR. To the extent that political consensus has determined that certain data processing activities must be deterred, there is little room for further debate. The results of these policy determinations have established a respect for privacy as a leading fundamental right.

But the GDPR leaves open many interpretative questions, and although efforts by data regulators are underway to provide guidance, privacy professionals continue to struggle to provide clear operating instructions to senior executives who face the risk of stiff penalties in less than a year. For organisations planning to implement the GDPR, even more concerning than the spectre of penalties is the inability to know today whether data-dependent products and services already (or about to be) deployed will be on the right side of an evolving body of law.

Policymakers on both sides of the Atlantic have a firm interest in helping support a digital ecosystem that protects individuals while enabling data-driven advances. But the path to compliance with the GDPR's strict set of limits may be rocky. The risk is that when coupled with uncertainty over its interpretation the GDPR, with its steep penalties and conflicts over its interpretation, could widen the EU-US divide. These days, global companies are deploying teams of technologists, lawyers and privacy experts to address these new challenges. Hopefully, their efforts to do so will enhance trust in the digital economy while also strengthening the deep mutual values that citizens and consumers so cherish in both Europe and the US.