Expert Q&A: European Data Protection Supervisor on Digital Ethics

PRACTICAL LAW DATA PRIVACY ADVISOR

Search the Resource ID numbers in blue on Westlaw for more.

An Expert Q&A with European Data Protection Supervisor Giovanni Buttarelli on digital ethics, enforcement of the General Data Protection Regulation (GDPR), the role of the Information Commissioner's Office in the European Data Protection Board post Brexit, the status of the E-Privacy Regulation, and the California Consumer Privacy Act 2018.

Practical Law Data Privacy Advisor asked European Data Protection Supervisor (EDPS) Giovanni Buttarelli to discuss digital ethics, enforcement of the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), the role of the Information Commissioner's Office (ICO) in the European Data Protection Board (EDPB) after Brexit, the status of the proposed E-Privacy Regulation, and any advice he has to regulators about the California Consumer Privacy Act 2018.

GDPR

WHAT IS THE EDPB'S VIEW ON THE APPLICABILITY OF THE GDPR TO NON-EU GOVERNMENT BODIES?

The GDPR does not apply to non-EU established government bodies unless they process personal data about EU data subjects to either:

- Offer goods or services to EU data subjects, regardless of whether they require payment.
- Monitor their behavior in the EU.

Non-EU established private entities are more likely to meet these requirements than non-EU established government bodies. Non-EU government bodies should assess whether any GDPR requirements may apply indirectly. For example, where personal data is transferred from an EU established data controller or data processor to a non-EU government in a third country using the standard contractual clauses or binding corporate rules, the non-EU established government body may be required to respect GDPR principles.

For more information, see Practice Notes, Determining the Applicability of the GDPR (W-003-8899) and Cross-Border Transfers of Personal Data under the GDPR (W-013-9203).

WHAT HAVE WE LEARNED FROM THE PAST MONTHS OF GDPR ENFORCEMENT ACTIVITY?

The GDPR works. The nine months since the GDPR came into force demonstrates that. Organizations are no longer panicking and the GDPR proved that a two-year implementation period was sufficient to enable organizations to move towards compliance. Since May 25, 2018, EU member states such as the UK, France, and Portugal have issued the first enforcement actions (see, for example, Legal Update, ICO Issues First Enforcement Notice under GDPR (W-016-7589)). However, what is important is not the number of fines issued but the successful coordination between member state supervisory authorities (DPAs) with regard to the one-stop shop and consistency mechanisms and the GDPR's mutual assistance provisions. Of the six one-stop shop and consistency mechanism cases which have concluded, all have settled without the need to escalate to the EDPB for a decision. The statistics concerning the exchange of information between the DPAs confirms their commitment to speak with one voice and to be consistent and transparent in relation to how the DPAs will apply, interpret, and enforce, the GDPR.

Moving forward, the accountability principle should be better developed within organizations and DPAs should be less prescriptive. We need to trigger a new generation of culture in terms of awareness, training, and good practice.

For more information, see Practice Notes, Cross-Border Enforcement and One-Stop Shop under the GDPR (W-016-3325) and Demonstrating Compliance with the GDPR: Accountability and Demonstrating Compliance (W-005-2644).

EUROPEAN DATA PROTECTION BOARD (EDPB) AND THE INFORMATION COMMISSIONER'S OFFICE (ICO)

WHAT ROLE WILL THE ICO PLAY IN THE EDPB POST BREXIT?

The ICO is currently a full member of the EDPB. It is active with regard to certain binding corporate rules and standard contractual clauses cases and is the lead authority for important personal data

processing. It will be a huge loss if we no longer have the ICO's contribution post Brexit.

If the UK leaves the EU without a deal, our only option is to consider the ICO to be a supervisory authority in a third country which does not have an adequacy finding. Even if the UK achieves an adequacy finding in the future, the ICO will still be a supervisory authority in a third country. Supervisory authorities from third countries cannot attend EDPB plenary meetings.

There are many other opportunities to cooperate with ICO, for instance the Spring International Conference, the International Conference of Data Protection and Privacy Commissioners and the Executive Committee that the ICO leads, the Council of Europe, or in the international working group on cooperation they lead.

A no deal outcome will not be the end of bilateral cooperation between the ICO and the EDPS or other EU DPAs. I am sure we will continue working together in a different way.

For more information, see Practice Note, Brexit: Implications for Data Protection: Future Relations between the UK and the EU in Relation to Data Protection (W-016-7309).

DO YOU AGREE WITH THE ICO THAT THE BETTER EQUIVALENCY MODEL IS A FORMAL (RECIPROCAL) TREATY RATHER THAN A (UNILATERAL) COMMISSION DECISION?

The GDPR requires unilateral decisions that the European Commission adopts. However, that does not prevent creativity. The Japanese trade agreement did not contain data protection provisions but it is accompanied by two data protection adequacy decisions. The European Commission and the competent Japanese authority, which assessed the EU system, adopted these decisions in terms of reciprocity. I think this is the first time a third county has assessed the adequacy of EU legal system on data protection.

For more information, see Legal Update, EU and Japan Mutual Adequacy Decisions in Force for Transfer of Personal Data (W-018-6827).

E-PRIVACY REGULATION

WHAT IS THE STATUS OF THE E-PRIVACY REGULATION? WHEN CAN WE EXPECT IT TO BE IN FORCE?

There's still unfinished work with the E-Privacy Regulation, which will replace the EU E-Privacy Directive (Directive 2002/58/EC), as amended by the EU Citizens' Rights Directive (Directive 2009/136/EC), and that's a shame. To ensure the long-term success of the E-Privacy Regulation, we understand the need for further discussions on specific topics such as innovation, AI, and Big Data. However, we also need urgent solutions to reinforce freedom and security of communications. The current situation is not sustainable for data controllers that must respect the GDPR together with the electronic communication directives based on an entirely different regime.

I believe that the Romanian presidency at the European Council will succeed by early June in identifying solutions to the remaining concerns, before the presidency hands over to Finland.

For more information, see:

- Legal Update, EDPB Issues Statement on the Revision of the ePR and Its Impact (W-015-0824).
- Legislation Tracker, Digital Single Market Strategy: Regulation on Privacy and Electronic Communications (Eprivacy Regulation): Legislation Tracker (W-007-8182).

DATA ETHICS

WHY IS IT IMPORTANT TO DEBATE ETHICS WITH PERSPECTIVES FROM TECHNOLOGY CEOS, INTERNATIONAL JUDGES, HUMAN RIGHTS ACTIVISTS, JOURNALISTS, AND DATA PROTECTION AUTHORITIES? WHAT ROLES DO THEY HAVE TO PLAY?

Digitalization pervades all aspects of our lives as individuals and all sectors of societal organization. It changes the way we communicate, move, meet people, and collect information. It changes the way our medical files are stored, how streets and borders are controlled, how research is conducted. All of these changes come with a wide range of implications. It was therefore important to me, as the host of the 2018 International Conference of Data Protection and Privacy Commissioners (ICDPPC), to invite as broad a spectrum of stakeholders as possible. We wanted to have everyone around the table because everyone is affected and has to have a word to say in this debate.

Of course, we faced criticism for allowing Facebook and Google onto the stage, but we all know that they are among the most powerful players and need to hear and be confronted with our questions and concerns. Judges, human rights activists, journalists, and data protection authorities witness and observe the effects of new digital technologies on people's lives and on their fundamental rights. All of them have important perspectives to be heard in the debate towards a sustainable governance of digitalization. Moreover, we made sure to involve representatives from all geopolitical regions. In this globalized and interconnected world, only a truly inclusive conversation can lead to widely accepted ethical standards.

For more on the EDPS' work on digital ethics, see Legal Update, EDPS Publishes Summary of Outcomes of Public Consultation on Digital Ethics (W-016-8328). For more on the ICDPPC's conference, see: ICDPPC: Debating Ethics: Dignity and Respect in Data Driven Life.

WHAT IS THE BUSINESS CASE FOR STRONG DATA ETHICS? DO YOU SEE MORE BUSINESSES USING DIGITAL ETHICS AS A WAY TO DISTINGUISH THEIR GOODS OR SERVICES?

Indeed, privacy is getting "en vogue" for individuals and companies. With the adoption of the GDPR, but also with recent scandals such as Cambridge Analytica and problematic developments such as the roll-out of the social credit system in China, there is a whole new level of awareness around risks and dangers among the general public. More and more people are concerned about how their data is used. This is also why some businesses have started to develop better privacy standards:

- It is "in".
- It is an advantage in the market.
- It makes users choose your services over others.

While this is a welcome development, it is also important that companies develop a genuine ethics culture and understanding of the importance of behaving ethically: digital ethics, not because it is a competitive advantage, but because it truly matters.

WHAT GUIDANCE DO YOU HAVE FOR BUSINESSES THAT WANT TO IMPLEMENT OR EMBED BETTER ETHICAL PRACTICES? DO YOU PLAN ANY ENFORCEMENT ACTION IN THIS AREA?

Companies should step back and reflect on their role in society and how their products impact people's lives. For many, this will include a careful consideration of their business model. We have seen, for instance, that the monopolization of advertising is highly problematic, as it endangers the free press and can easily be abused to undermine democracy. Companies should:

- Take a broad view of their responsibilities.
- Invest in staff to rethink their functioning from an ethics-based perspective.
- Implement respective changes.

We cannot enforce ethical thinking, this needs to come from within and become the heart of any organization working in society. Let us ask ourselves again and again what change we want to see and how we can be that change.

WHAT'S THE DIFFERENCE BETWEEN DIGITAL ETHICS AND LEGAL DATA PROTECTION COMPLIANCE? IF AN ORGANIZATION COMPLIES WITH DATA PROTECTION LAWS, COULD THEY STILL ACT UNETHICALLY WITH DATA?

Of course they could. The GDPR is an important step forward but digital technologies will continue to evolve and laws will quickly become out of date. The GDPR focuses on individual rights. It does not consider the broader societal implications of new digital technologies.

Ethical thinking and deliberation come before, during, and after the law. Ethics are the foundations of our legal systems and ensure that they are updated when necessary. Debating ethics and discussing what is right and wrong is the process of societal self-reflection and self-evaluation on which we, as members of society, establish values and norms and enact binding, enforceable rules. This is where the difference between law and ethics lies. While laws are part of a society's ethics, their differentiating characteristic is that they are enforceable, that there is a public, official mechanism that holds you to account and sanctions you if you violate them.

History has shown that ethical notions of good and bad change. This means that they must continuously be re-debated and re-defined. Whenever technological innovation came with risks and dangers, ethics have been key in addressing and preventing them. Ethics can also help us now to find a path into a digital future that re-affirms and protects our long-standing culture of values and rights.

ARE THERE ANY PARTICULAR SECTORS OR INDUSTRIES WHO ARE ADVANCED IN THE AREA OF DATA ETHICS?

Over the last few years, more and more professional organizations have engaged in developing guidance on ethics, including the Institute of Electrical and Electronics Engineers (IEEE) Ethically Aligned Design or the Association for Computing Machinery's (ACM) updated Code of Ethics and Professional Conduct, which both place privacy at their core (see IEEE Standards Association: The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems and ACM: ACM Code of Ethics and Professional Conduct).

Companies and other stakeholders have joined in creating various platforms to discuss ethics, among them the Partnership in AI (PAI) (see PAI: About Us). Public institutions have also contributed strong guidance, including the ICDPPC's Declaration on Ethics in Data Protection and Artificial Intelligence recently adopted at the conference I had the honor to host, as well as our own publications, most importantly the recent EDPS Ethics Advisory Group's Report.

For more information, see Legal Updates, Data Ethics Developments: EDPS Publishes Report and Government Reaffirms Commitment to Create UK-Based Centre for Data Ethics and Innovation (W-012-8970) and Data Protection and Privacy Commissioners Adopt Declaration on Ethics and Data Protection in AI (W-017-2648).

WHICH SECTORS NEED TO IMPROVE IN THIS AREA?

Clearly all sectors need to improve and will always need to improve. As Professor Norman Sadeh said at our conference: "Ethics is not a destination, it is a journey." (For more information, see Debating Ethics: Norman Sadeh.)

DO INDIVIDUALS UNDERSTAND THE RISKS ASSOCIATED WITH A LACK OF DATA ETHICS? IS IT AN AREA OF CONCERN? HOW DO WE EDUCATE AND EMPOWER INDIVIDUALS IN THIS SPACE?

Societal awareness is indeed increasing and many people are getting more privacy-conscious. A recent US study says that since Cambridge Analytica:

- Over half of (adult) Facebook users have adjusted their privacy settings.
- Around 40% have taken a break from checking the platform for a period of several weeks or more.
- Around a quarter say they have deleted the Facebook app from their cellphone.

(See Pew Research Center: Americans are changing their relationship with Facebook.)

Nevertheless, we often tend to succumb to the short-term benefits of services or apps and discount long-term risks. Behavioral studies prove this is a human cognitive limitation. Whenever profitable, we tend to go for the service and disregard its potentially problematic small print. So, yes, we need to continue raising awareness. But most of all, we also need to get the developers and providers to stop manipulating us (see Legal Update, EDPS Published Opinion on Online Manipulation and Personal Data (W-013-8646)).

Professor Sadeh, one of the panelists at the ICDPPC, pointed to the language used in many privacy settings. He said, if you ask users to agree to certain privacy settings because they will benefit from it for reasons that you then list, most of them will opt in. If you tell the users that you would like to track their location because you want to mine it, find out more about their lifestyle and their preferences, sell information about them to others, you might get another answer. Law and philosophy professor Anita Allen, one of our keynote speakers, also said that the 21st century has added an unprecedented complexity to ethics and technology. Therefore, it is understandable that ordinary people are overwhelmed by the speed of innovation and underinformed or confused about the facts they would need to live well and responsibly with new technologies (see Debating Ethics: Anita Allen).

So yes, we need to empower individuals to take well-informed decisions, most of all need to create an ethically conscious production sector. Innovation must be responsible. Only then will it be true, sustainable innovation.

HOW DO YOU ENFORCE DIGITAL ETHICS ON A GLOBAL SCALE? SELF-REGULATION AND CODES OF PRACTICE OR STRICT RULES AND ENFORCEMENT?

Both are necessary, and with the GDPR Europe leads by example and sets up a first set of globally binding rules. Of course, more will be needed, and professional codes and guidelines will play a crucial role as well.

WHAT ROLE DO YOU SEE FOR INITIATIVES SUCH AS THE UK'S CENTRE FOR DATA ETHICS AND INNOVATION OR THE WORK OF THE CANADIAN HOUSE OF COMMONS' STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS (ETHI)?

There are many excellent initiatives under way from both public institutions and professional associations. The more opportunities we create to discuss digital ethics, the faster we will move forward. Yet, we also need to bring all these different initiatives together and establish internationally recognized and respected standards for the development and deployment of emerging technologies.

For more information on the UK and Canadian initiatives, see Legal Updates, Government Responds to Consultation on Centre for Data Ethics and Innovation (W-017-6965) and Data Privacy Advisor Global Bulletin: January 30 to February 5, 2019: Canada: Privacy Commissioner Comments on ETHI Study on Privacy of Digital Government Services (W-018-7840).

WHAT CAN ORGANIZATIONS LEARN FROM FACEBOOK?

There are three lessons for any organization:

- First, your clients will lose their trust in you and leave you if you do not respect their rights and dignity.
- Second, you face sanctions and reputational damage.
- Third, your business model is not successful in the long-term.

So I repeat: real innovation is responsible innovation.

CALIFORNIA CONSUMER PRIVACY ACT 2018

WHAT LESSONS FROM THE GDPR DO YOU HAVE FOR THE CALIFORNIA REGULATORS OR FOR OTHER US STATES CONSIDERING SIMILAR LAWS?

We are closely following this interesting debate about the California Consumer Privacy Act's (CCPA) future. Many other US states have already started considering similar laws, which can be considered GDPR oriented, meaning GDPR-like or GDPR-lite (see CCPA Expansion Proposed, Data Privacy Monitor, February 27, 2019). This is an incentive for the US to explore the possibility of having a federal law. There is a public interest not to fragment data protection laws at the state level.

I would read the CCPA as a big incentive for a unique and needed approach, taking into consideration that now more than 120 countries in the world are equipped with a modern generation of data protection provisions, and more than 70 are outside the European geographical territory. Some of those provisions will allow the relevant countries to sign and ratify the modernized Council of Europe Convention 108. This means that GDPR has triggered a big discussion around the world.

For more information, see Practice Notes, CCPA and GDPR Comparison Chart (W-016-7418) and Understanding the California Consumer Privacy Act (CCPA) (W-017-4166).

03-19