Privacy and data protection

Venture into the future of privacy

Kristina Irion
Institute of Information Law at the University of Amsterdam, Department of Public Policy at Central European University (Budapest)

At the time of writing, I am at the Computer Privacy and Data Protection Conference in Brussels, for insiders just CPDP 2015, one of several mega-events with more than 1,000 participants from governments, European Union (EU) institutions, corporations, civil society and privacy advocates, and plenty of lawyers and academics just like me. This is emblematic of the transformation privacy and data protection have undergone from a somewhat dull area of law to a very visible cutting-edge legal expertise.

Privacy is sexy!

This clearly is a reflection of today's data-driven environment requiring experts in privacy and data protection. For lawyers this field is attractive because it cuts across many different disciplines, such as fundamental rights, EU law, national data protection regulations and contract law, always against the backdrop of the latest developments in information and communications technology. Moreover, there is also a generation of young female lawyers rising who specialize in information privacy law. The prospects for young professionals in data privacy are golden at the verge of cloud computing, big data, mass surveillance, the internet of things.

Legal education in privacy law and policy is still not up to speed regarding the demands. As a subject, privacy and data protection leads a niche existence in specialized master programs at a dozen or so European universities. The fundamentals of legal protection of personal data flows have not yet entered the curricula of legal bachelor education in spite of its societal relevance. At the same time, law students can be introduced to this field once they have acquired a sound knowledge of the cross-cutting disciplines that are highlighted above.

The privacy paradox

With its high legal standards in data protection, the EU is on the one hand a global frontrunner and at the same time put on the spot as to whether its approach is workable and effective. The legal concepts that carry the EU approach to privacy and data protection are under considerable strain because they were not conceived for the ubiquitous use of personal data and their global flow that is the prevailing paradigm in today's world. Paradoxically, it is possible to comply with EU data protection regulation (Directive 46/95/EC) in such a way that systematically undermines its very aim, that is, to protect the fundamental right to privacy and to equip individuals with effective means to decide who is permitted to use their personal data for what purposes exactly.

A regulatory approach that aims to harness individuals' autonomy does not stand a chance against business models that involve the extensive collection of personal data. This is true for the personal information we actually volunteer when we use online services (social media or share user-generated content) and even more so for all the infor-

mation that emerges as a by-product of our hyper-connected lives. Contrary to consumer protection law, data subjects who have to give their consent to the processing of personal data are deprived of the safety net of unfair commercial practices and collective bargaining vis-à-vis the corporate giants, such as Google, Facebook and Microsoft, to name just a few.

Weaving a personal data threat

The information revolution goes hand in hand with an unprecedented explosion of data. The Internet of things is about to integrate offline and online through smart devices (e.g., phones, cars and homes) that operate in smart environments (e.g., cities, grids, health care and traffic). In many respects, such information-driven activities contribute to benign progress that benefits individuals, society at large and the natural environment.

This is the right moment to invoke the silkworm analogy Chris Marsden and Ian Brown introduced in their book "Regulating Code: Good Governance and Better Regulation in the Information Age."[1] Both silkworms and humans have in common that they involuntarily produce a valuable raw resource. Caterpillars create cocoons from silk fibers that are used to make a luxury cloth. Humans generate a personal data trail as a by-product of their multifarious online activities that

“ Contrary to consumer protection law, data subjects who have to give their consent to the processing of personal data are deprived of the safety net of unfair commercial practices and collective bargaining vis-à-vis the corporate giants, such as Google, Facebook and Microsoft, to name just a few.

vastly exceeds the personal information we actively volunteer in online transactions.

The value that companies attach to click-stream and metadata is immense because it holds a more granular picture of individual activities that can be used to understand us better as consumers. This is a most emphatic way to frame processes known as monitoring, profiling, data mining, behavioral targeting and predictive analytics of our potential as consumers. Individuals are often not aware of the hidden face of online personal data processing and they have little to no means to influence how their personal data is used and shared but should have confidence that everything happens in propriety and good faith. This blanket approach

1. The catching silkworm analogy I borrowed from Chris Marsden and Ian Brown's book "Regulating Code: Good Governance and Better Regulation in the Information Age" (Cambridge MA: MIT Press, 2013).

to trust, however, is not suitable to empower individuals and more likely to undermine consumer confidence.

Weaving smart data protections into the texture of the right to privacy

In a sense, the caterpillars are better off because after their metamorphosis they rise as moths into a new life cycle leaving their silk cocoon as debris behind (if they are not part of those unfortunate ones that only live for silk production.) The personal data trail, however, would stick with the individual forever save when legislation sets limits. In its widely discussed 2014 judgment, the Court of Justice of the EU found in favor of a right to be delinked from search engine results (sometimes wrongly referred to as a "right to be forgotten") in the case of name searches (*Google Spain SL*, C-131/12). This is a fine example of how progressive jurisprudence can interpret data protection regulation.

As one of the key actions, the 2010 Digital Agenda for Europe proposed a review of the EU data protection rules and the EU legislators are about to finalize this year a new regulation which would unify data protection rules throughout the internal digital market. There are a number of important regulatory innovations in the proposal and overcoming the present legal fragmentation would already mean an important improvement.

However, the proposal by and large extrapolates the concepts of the 1995 Directive into the future without adjusting the approach to ubiquitous data processing or significantly strengthen individuals' data protection rights. Missing from the proposal are scalable regulatory instruments that would relieve individuals from the burdensome micromanagement of their privacy and data protection through consents and personal settings. In order for privacy to persist in the future, individuals should be able to set preferences on their end that would be effective across services, devices and providers.

Governments, too, take a toll on citizens' privacy

Moreover, government bodies that can practically authorize themselves increasingly pass legislation that enable authorities to process the personal data of citizens for a variety of purposes. Which public service today can really subsist without data processing? While this is done in pursuit of the public interest, public authorities are under an obligation to meet the standards of national constitutions and European fundamental rights, as applicable. And the real challenges are how to tailor the actual scope and extent of personal

> **"In order for privacy to persist in the future, individuals should be able to set preferences on their end that would be effective across services, devices and providers.**

> **“ The ensuing question is how much public services should be personalized or whether there are fair solutions that would be less invasive of privacy but serve equally well the public interest?**

data collection and use to serve the public purpose without exceeding the limits of what is necessary and proportionate in the light of the legitimate objectives pursued.

In practice, it will often be the case that more data produces more accurate measurement, for example when levying road tolls, garbage fees, or using public transport, to name just a few examples. The ensuing question is how much public services should be personalized or whether there are fair solutions that would be less invasive of privacy but serve equally well the public interest? Moreover, personal data collections always risk a mission-creep when this data would be used for a new purpose different to the one for which it was originally collected. Just think of automated number plate recognition used in some countries to collect road tolls. The same infrastructure could be repurposed to search for stolen vehicles or criminal suspects. This means difficult tradeoffs have to be made between fundamental rights and values on the one hand and on the other hand security in order prevent a democratic and open society to gradually slide into a surveillance state.

Especially in the field of national security and law enforcement, the right measure can be easily missed as we learned from the Snowden revelations about mass surveillance of online communications by U.S. and European countries' intelligence agencies. In their fight against international terrorism and serious crime, governments are very prone to prioritize measures that amount to heavy privacy invasions, such as the indiscriminate retention of metadata about everybody's electronic communications. In a recent judgment, the Court of Justice of the EU invalidated the notorious 2006 Data Retention Directive (*Digital Rights Ireland and Seitlinger*, C-293/12 and C-594/12) because it imposed intrusive mandatory data retention schemes without affording sufficient protection to the rights to privacy and data protection.

Above all, it should not be forgotten that defending privacy is not only about individual fundamental rights but about preserving the societal conditions for a range of other fundamental rights and democratic values to flourish. Without it, citizens could not freely express and inform themselves, form associations and political beliefs, hold free democratic elections and hold their governments accountable. Without it, consumers cannot make informed decisions, users are at the mercy of their digital shadows and in general disempowered in the information-driven economy. And now its time for you to search for your fellow law student Max Schrems from Austria in order to discover what a modern-day legal adventure privacy and data protection can be.