

OPINION: EU CLARIFIES PARAMETERS OF DATA PROTECTION

The European Union's General Data Protection Regulation, due for adoption this year, is intended to harmonise data protection laws across the EU. Burkhard Schafer, Professor of Computational Legal Theory at the University of Edinburgh, outlines the key points and comments on the engineering implications and legal ramifications of the new regulatory regime.



Professor Burkhard Schafer

The growing globalisation of data flows and the ever-increasing capabilities of big data analytics increase the risk that people can lose control of their own data. The new EU regulation "on the protection of individuals with regard to the processing of personal data and on the free movement of such data", expected to be agreed between the European Commission, Parliament and Council during 2015, aims to strengthen the protection of "data subjects" – citizens whose data is collected – while enabling growth in the digital economy.

The regulation represents the most significant global development in data protection law since the EU's Data Protection Directive of 1995. The legal framework of the earlier directive has struggled to remain relevant in an age of mass information sharing. The Commission itself has described the current situation as one of "fragmentation and incoherence".

The new regulation does not require implementation by member states and will be directly applicable law. Instead of dealing with 28 separate national data protection

regimes, once a company is compliant with the regulation's rules, it can carry out business throughout the EU. All companies offering goods or services in the European Union will be subject to the same data protection rules, regardless of where they are based. This harmonisation comes at a cost, with rules that are in many respects more demanding than those in the present directive. Businesses will be given only until 2017 to adapt to this new environment before they face steep fines, possibly up to 5% of annual turnover, for noncompliance.

Why does this matter to engineers? For the first time, "privacy by design and by default" will be enshrined in law, turning engineering choices into legal mandates. In the future, almost every new product – from autonomous cars through to intelligent fridges to gaming apps – will require that data protection requirements are considered and built into the system already in the design stage. This evaluation will have to cover the entire product lifespan, from any initial "knowledge acquisition stage" through its use by customers to its eventual recycling.

The proposed regulation not only creates new legal rights for citizens; it also gives software developers and hardware engineers a pivotal role in their enforcement.

Creative and intelligent design and manufacturing solutions will be needed, including new ways to develop data mining algorithms that offer the same benefits to businesses while collecting less personal data than at present. New ways to build hardware will be needed that, for instance, limit what the sensors of a machine can see without reducing its performance significantly.

A short example can illustrate this point. In 2014, the Court of Justice of the European Union ruled in *Google v González* that Google was under an obligation to remove links to personal information, at the request of a data subject, provided the information is "inadequate, irrelevant or excessive". Google's response to this decision framed it as a traditional issue of legal compliance: the ruling was a potential interference with its business, to be complied with only to the degree mandated by law. One consequence, to the dismay of the EU, was to exclude the google.com domain from this process, arguing that the CJEU has no jurisdiction over the US part of its business.

The response could have been very different had Google framed the situation as an engineering challenge. Google's business is information retrieval (IR). Good IR does not retrieve everything, only information that is relevant, adequate and timely. Framed like this, the decision requires Google to remove only data that a 'perfect' IR algorithm would have excluded anyway.

'Perfect' IR algorithms are a difficult task for AI. Seen like this, Mr González and every applicant for link removal after him helped

Google improve its product by identifying potentially outdated information. People who own their data also curate it. Google's approach then could have been to make this new crowdsourced IR improvement as easy as possible and integrate it seamlessly into its data collection processes. This would also have sidelined the question of jurisdiction: The new product is better, not just EU law compliant, and thus of benefit for every user worldwide.

However, such a gestalt switch that sees Mr González not as a disruptive litigant, but a knowledge engineering resource, requires a new breed of lawyers. Traditionally, lawyers come in only after a data breach has occurred to attribute blame, or after a product is developed to express concerns. Now, they will need to understand enough engineering to suggest creative design and manufacturing solutions as part of harm prevention through technology, working closely with developers. Equally, it requires a new breed of engineers who understand enough about the law that it becomes for them almost like a material to work with. In other words, the regulation forces engineers and lawyers to work together in new ways to create systems that respect the individual's right to privacy while allowing new technologies to thrive.

Are we ready in the UK for this revolution in the way we think about the interaction between lawyers and engineers? There are

grounds for concern, mainly with regards to education, curricula design and training.

In the US, law degrees are postgraduate qualifications studied after completion of a degree in another field. This produces a much greater pool of lawyers with a background in science and engineering. Germany, by contrast, has its technical universities, powerhouses for technological invention and innovation. Lacking law schools, these universities embed instead individual law academics in informatics or engineering departments. This benefits curriculum design – engineering students will have been exposed at least to some legal training – as well as collaborative research and development.

In the UK, engineering and law departments often have little interaction. Working within these structures to ensure that we prepare the next generation of students for the radically changed legal regime will be a challenge. Professional bodies also have their part to play, not only through their influence on curricula, but also by formulating appropriate standards and supporting them through continued professional development.

The new regulation, rightly used, is an opportunity, not a hindrance. Under its regime, technology-savvy lawyers and legally aware engineers will be worth their weight in gold for technology companies across the world.

BIOGRAPHY

Burkhard Schafer is Professor for Computational Legal Theory and director of the SCRIPT Centre for IT and IP law at the University of Edinburgh. His main fields of interest are the interactions between law, science and computer technology, especially computer linguistics.