The Globalization of European Privacy Law?

AALS Panel

January 6, 2013

Remarks by Francesca Bignami

A major reform of the EU data privacy framework is underway. In these remarks I will focus on two sets of changes contained in the proposed legislation, one of which is specific to EU governance and the other of which is relevant for data privacy policy generally. On the first score, the most important trend is the centralization of power at the EU level, with a corresponding loss of power for national legislatures and national data protection authorities. On the second score, most of the changes that have been made to data privacy policy have brought the EU framework closer to the US one. In other words, EU and US regulatory policy are converging in important respects.

Background

The new EU privacy legislation was proposed in January 2012. There are two pieces of legislation: a Directive, which covers law enforcement activities by the police and judiciary; and a Regulation, which covers everything else. The most important is the Regulation and the bulk of my remarks will focus on that. These two pieces of legislation are now winding their way through the EU legislative process. They are to be adopted under the "ordinary legislative procedure", formerly known as "co-decision", under which the Commission proposes and the Council of Ministers and European Parliament each have an equal vote. The process is anticipated to take at least 2 years. As of yet, the legislation has been considered by committees of the European Parliament and the Council but has not been voted on in either body. After the

legislation is passed, there is a two-year window for implementation, at which time it will come into force in the Member States. The best guess is that it will come into force in either 2015 or 2016.

For those unfamiliar with the field, the privacy guarantees in both EU and US law can be traced to the Fair Information Practice Principles developed in the early 1970s. On the European side of the Atlantic, the FIPPs were codified in the Council of Europe Convention of 1981, which has, in turn, served as the basis for all of the EU legislation in the field. There were, and continue to be, four different types of guarantees: **oversight** of databases, **accuracy** of the personal data contained in computing systems, **data security**, and **limits** on the collection, use, and storage of personal information. First, through *oversight*, ordinary individuals are empowered vis-à-vis those who collect their personal data. Transparency is key to oversight: the existence and the inner workings of information systems are to be disclosed to the public. Access is also important to ensuring oversight: individuals have the right to request their personal information and, if necessary, to correct or erase that information. And in all European systems, independent data protection authorities have been established to enforce privacy guarantees. Second, the requirement of *accuracy* of personal data protects against unfounded and manifestly unfair determinations based on that data. Third, *security* prevents fraudulent uses of personal data stored. Fourth, *limitations* on collection, use, and storage deter governments and corporate actors from using personal data to violate basic liberties and controlling citizens.

Proposed reforms

How, then, does the proposed legislation innovate on the existing scheme, which is mostly contained in a Directive dating to 1995? As was mentioned at the outset, there are two distinct

aspects, one of which pertains to EU governance and the other of which concerns data privacy regulation more broadly speaking.

EU governance

On the first aspect, the proposed legislation would transfer significant powers away from the Member States and to the EU institutions in Brussels. The current directive, which had to be implemented by the Member States and gave rise to considerable variation in national privacy policy, will be replaced with a regulation, which has immediate effect nationally, and does not require implementing legislation. In other words, Member States will have far less discretion in how they give effect to EU privacy law and there will be considerably more uniformity among the Member States. Moreover, the legislation covering law enforcement will capture far more national police and judicial activity than previously: before it only covered exchanges of information between national authorities, now it covers all activity of national authorities. As for the day-to-day administration of the legislation, the European Commission would acquire significant powers. Under the current Directive, implementation is largely for national authorities and the Art. 29 Working Party, which is composed of national data protection authorities; under the proposed Regulation, the Commission would be authorized to adopt so-called "delegated" and "implementing" acts in an extensive array of areas.

Privacy policy

Turning to the different choices that were made regarding data privacy policy, they fall into two categories, one having to do with substance and the other with the regulatory instruments used to govern the policy area.

Substance

On the substance, the proposed regulation significantly curtails the use of consent as a basis for collecting and using personal data. One of the devices for limiting the use of personal data is to require a legal basis for the data processing-- that it be done for a purpose recognized under law. Traditionally, consent has been one of the main purposes: the firm discloses the intended use of the personal data and the consumer, before undertaking the transaction, agrees to the use of her personal data. This, however, has largely been recognized as an ineffective limitation, since no one ever reads the disclosures and consumer rarely have the choice to say no and take their business elsewhere. The EU's move away from consent has an important parallel in the US: the FTC has rejected the so-called "notice and choice" model that was popular in the late 1990s and, in its March 2012 report on best privacy practices, it recommends limits on the types of data practices to which consumers can consent. Another important innovation contained in the proposed Regulation is the duty to inform individuals if their personal data is stolen or inadvertently disclosed, thus improving the incentives to maintain good data security practices. This was openly borrowed from the US, where there are many states that require data breach notification. Two other changes that should be briefly mentioned are the "right to data portability" and the "right to be forgotten." The first right is designed to enable individuals to easily switch providers, by giving them a fast and simple way of transferring their personal data. The second is an extension of the earlier transparency and access guarantees designed to achieve oversight by individuals. It makes explicit the right of individuals to check on what information is being held on them and to have that information erased if it is no longer being held lawfully by the provider, for instance, if it is old data that no longer serves the purposes of a long-expired contract.

Regulatory instruments

Moving to the regulatory tools designed to implement privacy rights, the proposed Regulation continues with two important trends that have been underway in the EU since the late 1990s: first, it recognizes and promotes a variety of self-regulatory instruments; and second, it improves considerably the enforcement powers of data protection authorities. This dual trend is what I have called elsewhere "cooperative legalism": a regulatory style that relies both on significant initiatives from industry **and** on the threat of punitive enforcement by regulatory agencies. The self-regulatory instruments contained in the proposed Regulation are as follows: all public bodies and private entities with over 250 employees have a duty to appoint a data protection officer responsible for developing privacy practices and guaranteeing compliance internally; privacy by design, meaning that firms must build privacy into their new technologies and products from the very beginning, when such technologies are being developed; data protection impact assessments, meaning that firms have a duty to conduct impact assessments for uses of personal data that are considered risky, for instance the use of health data; industry codes of conduct; binding corporate rules that guarantee privacy when data is transferred internationally; and privacy seals to indicate that a firm follows good privacy practices and thus create an incentive for consumers to do business with them. All of these techniques are becoming extremely important on the US privacy scene as well: the March 2012 FTC report encourages firms to adopt privacy by design and to develop industry-wide self-regulatory codes; the FTC in a December 2012 workshop has promoted self-regulatory privacy codes of conduct for firms with that engage in cross-border transactions; and most large firms today employ a chief privacy officer.

As for the powers of national data protection authorities, which remain the primary enforcers of EU privacy law, they have been expanded considerably. The new Regulation elaborates their

powers in vastly more detail than the current Directive. Most strikingly, it specifies the administrative fines that must be available to national regulators to punish transgressions of the rules. Under the proposed scheme, administrative fines could range up to 2% of company's annual worldwide income, which for most national DPAs constitutes a radical increase of their fining powers and represents an attempt to force firms to take privacy regulation seriously and to deal with the rampant under-enforcement problem that prevails in many countries. Tough regulatory enforcement is believed to be a distinctive feature of the American regulatory style, part of what Robert Kagan has dubbed "adversarial legalism." In the area of privacy regulation, the FTC has such fining powers in dealing with breaches of the rules on financial privacy as well as children's privacy. Therefore, we see that on this score, there is convergence as well between the US and the EU.

In sum, it is unlikely that the United States and Europe will see eye-to-eye on privacy anytime soon. The most important difference that persists is at the level of constitutional law: in Europe, data privacy is everywhere considered a fundamental right, whereas in the United States, the Supreme Court has been very slow to recognize data privacy as equal to more traditional forms of privacy. And even when the Court has done so, as with last term's GPS case, the right continues to apply only against government actors. However, as I have sought to demonstrate here, the specifics of EU and US regulatory policy are converging in important respects. Therefore, it should become increasingly easy for individuals and businesses, and other entities with cross-border dealings to navigate the two jurisdictions and to satisfy the regulatory requirements of the two sides of the Atlantic.