TOP of MIND

INTERVIEW WITH CHRISTOPHER KUNER

Dr. Christopher Kuner is Professor of Law and Co-Director of the Brussels Privacy Hub at the Vrije Universiteit Brussel (VUB), and Senior Privacy Counsel in the Brussels office of Wilson Sonsini Goodrich & Rosati. He specializes in European data protection law and currently serves as a member of the European Commission's multi-sectoral stakeholder expert group to support the application of the EU General Data Protection Regulation (GDPR). Below, he argues that the GDPR will have global implications, and that recent controversies could be a watershed moment for data privacy.

The views stated herein are those of the interviewee and do not necessarily reflect those of Goldman Sachs.

Marina Grushin: Why has Europe taken such an assertive role in setting the bar for data privacy regulation?

Christopher Kuner: In Europe, there is a belief that the increased economic and societal importance of data processing warrants strong legal protection of individual privacy. Several developments over the years have reinforced this view, from technological progress to the security-related debates following 9/11. More specifically, however, I think Europe is being driven by a constitutional imperative to protect individual rights. As the amount of data processed online has increased, so has the desire to increase legal protections for them.

Since data processing is globalized, this protection can't just stop at Europe's borders. Europe has therefore asserted its global reach in an attempt to extend such protection beyond them. European policymakers are well aware of the impact of their regulation around the world. Europe is not a military superpower, but it is a regulatory one. For example, by one count, over 100 countries have adopted EU-style data protection laws. Just as the US sets the standard on a large share of financial and corporate governance regulation, Europe has become the global benchmark for data privacy.

> "Since data processing is globalized, this protection can't just stop at Europe's borders. Europe has therefore asserted its global reach in an attempt to extend such protection beyond them."

Marina Grushin: Why do you think the US has taken a less active approach to data privacy?

Christopher Kuner: When I entered this field in the '90s, Europe and the US were more or less equal in their degree of global influence on data privacy. But in recent years, the US has veered off in its own direction. At this point, it is practically a global outlier in that it has no horizontal, omnibus data privacy law at the federal level. There are sectoral laws, case law, and enforcement actions, but no overarching framework. I see several reasons for this. The US has historically favored self-regulation and a hands-off approach in order to avoid hampering innovation. And there is no clear consensus on how restrictive data privacy regulation should be. There is also a general feeling of legislative and political gridlock, which has made it difficult to achieve wide-ranging reform on almost any issue, data privacy included.

There are debates about which system—US or EU—is best and most effective; I think there are arguments to make on both sides. But the EU has the advantage of being able to offer others a clearly-defined model. No one that I talk to in other parts of the world outside Europe ever says, "Let's adopt the US approach." There really isn't an overall approach to adopt. And so the US has lost influence in data privacy over the years.

Marina Grushin: What happens when different countries' rules are in conflict?

Christopher Kuner: There are frequent legal conflicts between data privacy law and laws and regulations in other areas, and there is usually no legal formula for resolving them. In practice, each jurisdiction tends to give priority to its own law. Either the companies have to work something out with the regulators, or they just have to make a choice about which rules to follow. In making that decision, companies often choose compliance with the law with the highest penalties in order to avoid the greatest potential enforcement risk. Since the penalties for breaches of data privacy law are increasing dramatically, this just makes the choices that companies are faced with even harder.

Marina Grushin: The EU General Data Protection Regulation (GDPR) becomes applicable on May 25. How does it fit into EU objectives on privacy?

Christopher Kuner: The GDPR will be a milestone in data privacy around the world. It is the successor to the EU Data Protection Directive, which has been in place for 20 years now. So for the decades ahead, the GDPR will be the major piece of EU legislation dealing with data privacy. It applies not only to the private sector but also to government entities. And since so many countries around the world have adopted EU-style data

Allison Nathan | allison.nathan@gs.com Marina Grushin | marina.grushin@gs.com David Groman | david.groman@gs.com

privacy regulation, many of them will almost certainly adapt their laws to the GDPR. For instance, I spent some time in Asia recently, and there is huge interest in the GDPR there. It is really a global phenomenon.

Marina Grushin: There seems to be substantial concern about the much stronger enforcement embedded in the GDPR and what that could mean for regulated industries. Is that concern warranted?

Christopher Kuner: One of the weaknesses of the current EU regime has been weak enforcement. So, as you said, a key element of the GDPR is much stronger enforcement with much more significant penalties, both in terms of potential monetary fines and other types of injunctive relief. GDPR fines can be as high as 4% of a company's annual turnover, which would be quite a substantial amount of money for a major company. This has led to something of a panic, with rumors of mega-fines and the internet all but shutting down after the GDPR becomes applicable. But from talking with regulators, my sense is that they're going to be fairly careful and strategic in imposing penalties; issuing severe penalties in a few well-publicized cases is often sufficient to scare many other companies into compliance. The US Federal Trade Commission (FTC) has used this approach in the past, and I think the EU regulators will too. So, there will be a lot more enforcement with much stronger penalties, but I don't think there is any reason for companies to panic, either.

That said, even with these stronger enforcement mechanisms, regulators still face significant challenges in effectively regulating internet and other technology-related companies. The regulatory bodies tend to be under-resourced and understaffed. The GDPR requires EU countries to increase funding levels and add staff, but there is still no way any regulator could compete with a major multinational company in that regard. The regulators also lack technical personnel, which is a serious problem for enforcement. It is increasingly difficult to understand how technologies work without a computer science background. Even a relatively sophisticated regulator like the FTC, which has many more people with a technical background than the European regulators do, is often stretched thin.

Marina Grushin: Are certain types of companies more vulnerable than others to increased regulatory scrutiny of privacy practices?

Christopher Kuner: Ten years ago, I might have said that data processing is important for some companies or sectors but not others. Today, that is no longer the case. The value of data has grown for companies in almost every sector, not only in economic terms but as an important part of how they operate. That said, there are certainly some areas that stand out. In addition to the internet companies themselves, there are sectors that routinely process high-value or sensitive data; think of medical companies dealing with patient health records or pharmaceutical companies involved in drug trials. This is also true with regard to financial services companies, where there is a huge regulatory and reputational risk if data are lost or misused. So companies in these sectors are probably a bit more vulnerable. But again, data processing has become so ubiquitous that data privacy is now important for companies in every field.

Marina Grushin: Will the recent controversy involving Cambridge Analytica and Facebook user data have lasting implications?

Christopher Kuner: I get the sense that this controversy marks a watershed moment in the history of data privacy, perhaps comparable to the Snowden revelations in the context of law enforcement and intelligence. There has been no lack of scandals involving data privacy over the last few years, and I don't want to comment on the situation of a particular company. But the current controversy involving Facebook and Cambridge Analytica seems to have grabbed the attention of politicians and the public in a way that others haven't. During the Zuckerberg testimony, even some Republicans in Congress suggested a need for privacy legislation. So I think this moment may potentially lead to new legislation or other regulation. That might take a long time to percolate through the political process. But unlike past calls for federal US privacy legislation, which didn't get very far, I think the current discussions could mark the start of a longer-term shift.

"Unlike past calls for federal US privacy legislation, which didn't get very far, I think the current discussions could mark the start of a longer-term shift."

Marina Grushin: German regulators have recently linked Facebook's data harvesting to its market power in social media. Do you see data privacy and antitrust regulation becoming more interconnected?

Christopher Kuner: In short, yes. In the past, the competition authorities didn't look at data privacy and the data privacy authorities didn't look at competition; they didn't really know each other's areas. But now, they're starting to talk to each other and work together more. In Europe, we've seen a number of competition authorities getting interested in the potential for companies to use their power over data in anticompetitive ways. And data protection regulators have become interested in this too. The result has been a number of high-profile investigations including the one you mentioned. I know that the FTC and others in the US have also raised this issue, and I think we will likely see a trend of more regulatory activity focused on the anticompetitive use of personal data.

Marina Grushin: How do you expect the notion of privacy to evolve over the coming years? And how will data privacy concerns ultimately be resolved?

Christopher Kuner: I think we will see even greater tension between people's desire to enjoy the use of technology and their concerns about privacy. Technology develops very fast, and the law is always trying to catch up with it. One of the few solutions I see that has real potential to change things is to actually build privacy into technology. An interesting feature of the GDPR, for example, is that it includes the concept of "Privacy by Design", under which companies that design data processing products and services will have to build in privacy from the beginning, rather than just cleaning up the mess if there is some problem later on.

Besides technology, the only other solution is for countries to come to a global consensus on data privacy, but that is unlikely in the foreseeable future. A move towards a federal privacy framework in the US would be a positive step for eventually developing some sort of global agreement. However, privacy is culturally determined, and the way it is understood differs around the world. So I believe that many areas of data privacy will remain controversial, and I expect things to get messier before they get neater.