Brown University Cybersecurity News Podcast: Europe’s New General Data Protection Regulation. Are you ready?

ALAN USAS: Hello. Welcome to Brown University's cybersecurity news podcast. I'm Alan Usas, program director for Brown's Executive Master in Cybersecurity.

The European Union has a big new privacy law. Global information flows are burgeoning. U.S. trade with the EU is more than $2.7 billion per day. Deborah Hurley, adjunct professor of the practice of computer science at Brown University, Fellow at the Institute for Quantitative Social Science at Harvard University, and principal at Hurley Consulting is here to tell you about it. Deborah.

DEBORAH HURLEY: Thank you very much, Alan. I'm going to be talking to you today about the law that is called-- get ready for it-- the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The short name for that is the General Data Protection Regulation. But try to say that five times fast. So immediately an acronym has developed. And that acronym is GDPR. Although it sounds like a former socialist republic, GDPR is the acronym for this new law, the Data Protection Regulation. And I urge you to memorize it.

The Data Protection Regulation was adopted in late 2015, 2016, after years of negotiation and will enter fully into force in 2018. And everyone, including everyone in the European Union and the rest of the world, is going to be needing this 24 months to get ready for the commencement of this law.

What do people want, what do companies want, when they think about doing business, traveling around the world, and all the things they need? The things that companies desire are predictability, consistency, and uniformity. Tell us what the law is, and we'll comply with it.

When you think about international law, privacy law is over 40 years old, which is not known by many people. And it actually, in addition, is one of the most consistent bodies of international law in the history of international law. I would certainly say that it's in the top three. Why is privacy important? Why is it important to have these privacy laws, and especially ones that are regional and global?

I'll just mention a brief example, IPv6. IPv6 is the next version of the internet protocol. It's partly implemented. But when IPv6 is fully implemented, one of the main drivers for its creation was to provide enough unique address space to assign a unique IP address to every molecule on earth up to one kilometer off the planet. So in the ubiquitous information environment, I'm going to wager we will use all of that address space as we embed computing everywhere, in the air, in solids, and in liquids.

In Europe, the driver for the new GDPR, the new General Data Protection Regulation, was the creation of the single market-- so the single digital market-- to help make European countries and the EU in general more competitive. The EU has been, since 1989, the global epicenter of privacy law around the world. And in 1989, they issued a draft directive, which was the first European regional law.

And historically then, it has been the center. As Eastern European countries were liberated, or liberated themselves, they looked to the EU for their laws-- also as Asia has developed, and so forth. So that has been the global epicenter and remains that.
I want to talk briefly about who the winners and losers are with regard to this new data protection regulation. In Europe, there are certainly winners, but it's an incremental win. It's not a huge win, an incremental win, because European countries and the members of the EU already have data protection laws and quite robust legal regimes and institutions. But there is an incremental win there, while they go to the regulation.

And one of the reasons for the regulation is to further harmonize the laws across Europe in pursuit of, or in furtherance of, this digital single market. So there's a huge practical job to be done in these 24 months. That's why there's a delay for the implementation of the full entry into force. In countries in Europe, there are literally hundreds of laws that will have to be reviewed in each country to make sure that it's compliant, to amend it, and so forth.

Another huge issue in Europe, with regard to privacy, although we hear a lot about it currently in the United States-- is their intelligence services. And they really have to deal with the issue of protection of data and privacy vis-a-vis their own national intelligence services.

Finally, as I mentioned, there's going to be an amendment of many, many laws in many countries. So literally hundreds of laws per country will be reviewed and maybe amended. So just to give you an example of the seriousness with which this is being taken in Europe, the CNIL, which is an acronym for the French Data Protection Authority, announced that they are beginning, because of this movement toward a single regulation and more uniformity in the laws in Europe, that they are actually commencing to offer all staff in the CNIL English language lessons on site to better prepare them to be able to cooperate with their fellows across Europe. So for a French authority to offer English language lessons on site is a cultural statement in itself.

In terms of countries like Canada, Australia, and New Zealand, which already have data protection laws, again, it's an incremental gain for them and for their population. In Latin America, there will be laws amended. Spain led a big initiative in the '90s to bring Latin American countries on board in terms of data protection. So they are part of the 100 plus countries around the world that have data protection laws. So again, there will be some amendment there, because trade with Europe, as it is with the United States, is very important.

In Asia-Pacific, Japan has a new law as well and also a new data protection authority that just went into effect in 2015. A very significant develop in Japan. So, some minor incremental changes there. China is increasingly a large trading partner with Europe and wants to increase that trade dramatically. So they don't have a data protection law. We'll have to be looking seriously-- and I know the Europeans will pressure the Chinese in diplomatic negotiations -- to adopt a data protection law.

China is still far from that. There hasn't even been a draft. But a country like India, which already has had a draft bill for a number of years circulating, is a good possible win in terms of increasing data protection around the world and would bring a billion plus people under the data protection umbrella.

The place that is actually positioned to gain the most from the European regulation is the United States and the Americans in the United States, the residents of the United States. US companies, for decades, because they have complied with these 100 plus data protection laws around the world, have been in the ironic position, or we've been the ironic recipients of their position, of protecting the privacy and personal data of non-Americans much better than they've protected the privacy and personal data of Americans.

So again, companies want uniformity, consistency, and predictability. They don't want to violate the law. Tell us what the law of Germany is, and we will follow it. If Proctor & Gamble didn't find it profitable to be in Germany, they would no longer be there. But for decades, they have. And you can be sure that they are complying with the data protection laws of Germany.
So actually, it's Americans who tend to or may benefit, be one of the largest beneficiaries of this new European regulation, as American companies raise their level of data protection overall. And that will also affect Americans.

We have, in the United States, the FTC, the Federal Trade Commission, which looks after some privacy issues. I call them necessary but not sufficient, because they don't cover all privacy issues. We certainly need a data protection authority in the United States. We don't have one. There is no homologue to that independent ombudsman that most countries in the world or at least half of them have to look after privacy and data protection.

And in fact, the United States did have, at one point, a proto data protection commissioner under George Herbert Walker Bush. There was a lovely woman who was a political appointee of George Herbert Walker Bush, who served out of the White House. She had an office in the White House and looked after privacy issues and attended international meetings representing the United States. So there's actually some small precedent for that.

This is absolutely a geopolitical issue. And we'll certainly be hearing more about it.

ALAN USAS: Thank you, Deborah, for the thorough explanation. In closing, are there some upcoming trends that you'd like to highlight?

DEBORAH HURLEY: Yes, indeed. I think the regulation is certainly going to be a dominant factor and everyone will be looking to it. If you haven't read it already, I urge you to take a look at it. But there are other trends as well that are really pushing the area of global privacy protection and providing both pressures and remedies for it. I'll just mention a few in particular.

One is the cloud, where we have a system where data is literally flowing all over the world. And the additional situation, where we don't know where the data is. The data's dynamic. That's part of the design of the cloud. And so there's a question where laws and regulations are and have been jurisdictionally -- and that means geographically -- based, when you don't know where the data is -- the data is dynamically moving -- then it becomes a question: well, how do you decide whose laws apply or which law is going to protect it?

So that leads to the resurgence of the field of privacy by design. So for decades, there has been a search for privacy by design or what are called privacy enhancing technologies, technical measures that could be used to protect privacy. So there was some activity there. Then it sort of faltered. But now there's a real resurgence, both because of the growth of the technology, in terms of big data itself becoming more real to people, these incredible global data flows, but also the growth of the technology and concomitant declines in cost have enabled certain technical measures that really weren't possible before.

Finally, there's an increasing move toward standards. So again, if you have international standards, those can be adopted by the private sector, by governments, and so forth. And they become an international norm over and above the legal standards.

ALAN USAS: Deborah, thanks again for sharing your thoughtful perspective on this new EU-US regulatory framework and its impact on the larger industry privacy debate. In future podcasts, we'll share more viewpoints on this and other cyber issues. For information on future podcasts, program news, and upcoming events, visit brown.edu/cybersecurity.