Why the EU's GDPR is critically important to everyone in the world – not just in the EU

Dr. L. Anne Breene, ArcoLogix

The European Union's General Data Protection Regulations (GDPR) went into effect on May 25, 2018. Any company doing business in the EU must implement GDPR with its EU clients, including companies in the US. Machine Learning (ML), as well as any resulting Artificial Intelligence (AI), are greatly affected by these regulations. The EU rules recognize that the methods of AI can influence us in powerful and sometimes dangerous ways. Even those who develop and implement AI often cannot fully explain or precisely predict how and why AI will work in a given situation, and this can lead to unanticipated results. As a first step toward controlling possible negative or unintended harmful consequences of AI, EU authorities have legislated that all users in the EU have the right and must be given the opportunity to: (1) opt out of automated decision making, (2) be provided with explanations of any such automated decisions and (3) have the results of an automated decision guaranteed to be free of prejudice of any kind. This legislation affects AI processes ranging from a credit decision to a Facebook algorithm that steers a viewer to a particular political article. Since the primary business model of the Internet at present is the gathering and analysis of personal information in order to present targeted, and theoretically more effective, advertizing, the implications to the industry are staggering.

Our 2016 presidential election was influenced by AI methods. Cambridge Analytica, the firm that applied AI methods in that election using data stolen from over 90-million unsuspecting American Facebook users and their friends and families, was spectacularly successful in its effort, but was forced to declare bankruptcy when public outcry caused its other clients to flee any association with the company. Cambridge Analytica is in process of rebranding and relocating itself – the technology of AI is simply too valuable to prospective customers to "put the genie back into the bottle". And Cambridge Analytica's activities were in addition to the use of email taken by suspected Russian hackers from the Democratic Party and others.

Nevertheless, even though Facebook must implement the GDPR consumer protections for its clients in the EU, Mark Zuckerberg has decided that Facebook will not do so in the US and Canada, the economics of Facebook's global business model, like that of many other ad-based Internet companies, is based on extensive data gathering and the application of AI to the presentation of ads and information. The resulting profits are just too large to abandon. Facebook's only concession to protecting customers is its statement that it will ban "hate speech" (which it cannot yet define), and that it will attempt to identify and remove the Russian bots from the US Facebook domain. In a recent full-page ad in the NY Times (May 27, 2018), Facebook proudly proclaims that "Together We Can Fight False News", but then leaves responsibility for doing so almost entirely up to the user. All that Facebook does is to provide a list of things the user can do to spot "Fake News". Why doesn't Facebook implement these practices itself? Because if it does so, it would have to refuse these ads and forego the revenue. "Helping" the user to spot these ads by themselves enables Facebook to look good while still running the ads and keeping the revenue.

The Congressional hearings with Mark Zuckerberg made the difficulty of controlling the improper use of AI technology extremely clear. Few in Congress understood the implications of the technology; most did not. And no one in Congress was permitted to analyze the details of the technology itself; since Facebook never released the actual algorithms it employs millions of times every day on its billions of users, so experts could never truly begin to assess the risks.

The following is an excerpt from a white paper that was recently published by the Continental Automated Building Association (CABA), that I co-authored. That paper "Artificial Intelligence and the IoT Connected Home," discusses some of the benefits as well as the dangers inherent in the use of AI in our homes. It is but one small part of a massive issue that can ultimately impact everyone on the planet in every aspect of their lives.

Even more compelling however are the European Union's General Data Protection Regulations (GDPR) that go into effect on May 25, 2018. Although, "the bulk of the language deals with how data is collected and stored, the regulation contains Article 22: Automated individual decision making, including profiling, potentially prohibiting a wide swath of algorithms currently in use in recommendation systems, credit and insurance risk assessments, computational advertising, and social networks, for example."[47] As well, the GDPR asserts that "Citizens have the right to receive an explanation for algorithmic decisions."[48] Since, "ML depends upon data that has been collected from society, and to the extent that society contains inequality, exclusion, or other traces of discrimination, so too will the data."[49] ***This boils down to the following: "black box" techniques as well as some supervised techniques that are using data collected from society and for which no measures have been taken that provably remove any discrimination, will not be allowed.*** Any US company with EU clients will be obliged to honor these regulations.

[47] Goodman, B. and Flaxman, S. 2017. European Union Regulations on Algorithmic Decision Making and a "Right to Explanation". AI Magazine 38(3): 50-57, *Association for the Advancement of Artificial Intelligence*. p. 51.
[48] Ibid, p. 51.
[49] Ibid, p. 53.

Today in the US, there is only one piece of legislation that protects any of our personal data - the **Health Insurance Portability and Accountability Act**, a law passed in 1996 designed to provide privacy standards to safeguard patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers. In the 22 years since then, there has not been one law passed to inhibit cyber-warfare that uses the private data of individual US citizens.

We in the AI field in the US must follow the lead of the EU in GDPR and forcefully make our voices heard about methods needed to keep our citizens, ourselves, and our democracy, safe in the future. Action is urgently needed on this front.

.

The white paper can be found at this link:
http://www.caba.org/CABA/Research/White Pa pers/FastForms/WH ITEPAPER/CABA WH ITEPAPER NOLOGIN .aspx?I D=2