Editor: Charles Petrie • cjpetriejr@gmail.com

Protect Data, Not Algorithms

Charles Petrie • University of St. Gallen, Switzerland

An interesting article in *Wired* reports on the coming collision between the AI in companies such as Google and Facebook and European law.[1] In this case, I'm on the side of the big companies.

The European Union's (EU's) current proposal to make it a right to get an explanation of how an algorithm used your data is a great example of why laws about computers shouldn't be made by bureaucrats who are computer illiterate.

First, what counts as an explanation in any case, much less to do with computing? There's no agreed-upon objective meaning for this. If someone asks you for an explanation, and you say something that makes them say "oh" and go away, that's the best we can hope for. Except, of course, that's not entirely true.

If you're teaching someone to perform a task, you might explain something to them, or ask them to explain, as part of the teaching process. Your explanations are successful if the student eventually performs the task correctly on their own. But I don't think that's what the EU has in mind.

So, a priori, a law requiring explanations is, shall we say, flawed. But a law requiring an explanation of an algorithm is so deeply flawed that the chasm is interesting to explore.

Suppose the algorithm is logic-based. How many people would understand an explanation of that algorithm? Some well-educated people would – but again, I don't think this is what the EU has in mind. Suppose it's based on statistics? Suppose, in fact, that it's based on any number of ways of computing similarity (such as those discussed by Ning-Han Liu in *Applied Intelligence*[2])? Would this count as an explanation under EU law: this music is similar to other music you have liked, and/or similar to the music that people like you liked. Or must the algorithm be described, along with all of the data used to compute the similarity? Really?

As the *Wired* article points out, it's even worse with neural nets, increasingly used by large companies. There's no explanation possible.

The only thing a company could do is explain to the individual how neural nets work, which is probably a lengthy explanation. Even lengthier would be the history of training instances and data used by the particular neural net in question. Still, I suspect the average Web user would feel the company isn't answering the question of how the current decision was made about them, but rather baffling them with long technical descriptions.

They would be right. Neural networks have been as successful in the last decade as they were previously unsuccessful, due to advances in using deeper layers as well as faster computers. But the essential disadvantage of this method of computing is that while there's science behind the technology, none of the individual results are scientific, but rather only engineering successes.

Science requires explanations with predictions that can be tested under repeatable conditions by other scientists. We call these *theories*, which can accumulate confirming evidence or be disproved.

The only theory we can have about a neural net that has learned to perform a task is that, in a particular case, the training data are sufficient to produce results we recognize as good, because presumably someone else could take the same technology and data, repeating the experiment with the same results. Yes, there's some science, such as postulating better results with more layers (or kinds of layers), but such a theory isn't the kind of explanation for which the EU law is asking.

You can't dig inside the neural net and come up with a repeatable logic that you can use to explain its behavior. A person can't publish a

1089-7801/16/$33.00 © 2016 IEEE

paper that says that such and such a logic will repeatedly produce such and such a result, except with regard to the underlying general computing mechanism. Specific results are a modern miracle. You can't explain miracles.

With neural networks, the EU law would result in companies pulling out of the EU, because they couldn't comply with it, in principle. Someone simply can't explain the particular weighting of neurons in various layers that result in the decision that resulted. There's no explanation to be had.

This EU law has gone wrong in a fundamental way. It goes down the terribly steep and slippery slope of asking companies to explain their algorithms. Apart from legal questions of trade secrets (even when there's an explanation to be had, of some kind), most consumers wouldn't understand it. If your bank starts using blockchain technology (from Bitcoin) to share your financial data, do you care? Well, okay, readers of this column do, but most consumers wouldn't — and moreover, they really shouldn't be involved so deeply in the bank's business.

I've previously offered a proposal for distributed data that would allow individuals control over how their data were used.[3] If implemented "correctly," it would also provide the so-called "right to be forgotten" that's a part of European law, as well as privacy.

And if you control your data, you control their use by any algorithm. That's the right level of consumer control. Trying to control all of the algorithms used to process data on the Web is futile. Asking for an explanation of the result of using the algorithm is simply the result of extremely shallow thinking about the issue.

The EU would do better to take a step back and focus on who owns data about an individual and how much control an individual has over that data. Then they would be on solid ground instead of a computing quagmire.

References

1. C. Metz, "Artificial Intelligence Is Setting up the Internet for a Huge Clash with Europe," *Wired*, 11 July 2016; www.wired.com/2016/07/artificial-intelligence-setting-internet-huge-clash-europe.
2. N.-H. Liu, "Comparison of Content-Based Music Recommendation Using Different Distance Estimation Methods," *Applied Intelligence*, vol. 38, no. 2, 2013, pp. 160–174; doi:10.1007/s10489-012-0363-y.
3. C. Petrie, "The Proper Use of the Internet: Digital Private Property," *IEEE Internet Computing*, vol. 20, no. 2, 2016, pp. 92–94; http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7420523.

Charles Petrie teaches and coaches the topic of innovation in design thinking at the University of St. Gallen, Switzerland (http://dthsg.com/dt-at-hsg/). He retired as a senior research scientist from the Stanford University Computer Science Department. His research topics are concurrent engineering, enterprise management, and collective work. Petrie has a PhD in computer science from the University of Texas at Austin. He was a founding member of the technical staff at the MCC AI Lab, the founding editor in chief of *IEEE Internet Computing*, and the founding chair of the Semantic Web Services Challenge. He also manages the Black Rock City Municipal Airport 88NV. Contact him at cjpetriejr@gmail.com.