GDPR's Right to Explanation: Pros and Cons

Though the European Union's General Data Protection Regulation (GDPR) is designed to push companies toward better information security, it comes with potentially unintended consequences.

As has happened with other security regulations, the language in GDPR leaves room to disrupt how companies do business.

Right to Explanation

One example is GDPR's "right to explanation," which will affect algorithms that make decisions based on user behaviors. Under the provision, a user can ask for an explanation about an algorithmic decision made about them.

On the surface, that sounds like a terrific idea. Who doesn't want to know what companies are collecting about them and why? Who hasn't been annoyed at some point about ads that cater to their interests to the point of creepiness?

The problem, some believe, is that it's impractical – impossible, even – to explain every decision made by algorithms, including those at the heart of many security programs. In other words, it opens up a can of non-ethical issues and can cause as much trouble for security as it's meant to solve.

Impractical and impossible

Nick Wallace, a Brussels-based senior policy analyst with the data policy think tank Center for Data Innovation, explained the problem as he sees it in an article he wrote in January for TechZone360. Among other things, he wrote, the right to explanation will do little to help consumers and will hobble the development and use of machine learning/artificial intelligence tools by holding developers to a ridiculously disruptive standard:

"Those who drafted the GDPR do not seem to understand that it is often not practical, or even possible, to explain all decisions made by algorithms. For example, autonomous vehicles are controlled by a multitude of algorithms that make many kinds of decisions. It is possible to log these actions, but it would take hours of work by highly-paid data scientists to render them intelligible. Often, the challenge of explaining an algorithmic decision comes not from the complexity of the algorithm, but the difficulty of giving meaning to the data it draws on."

He wrote that the regulation should be amended before the Right to Explanation piece stifles artificial intelligence programs and their myriad social and economic benefits.

The problem, some believe, is that it's impractical – impossible, even – to explain every decision made by algorithms, including those at the heart of many security programs. In other words, it opens up a can of non-ethical issues and can cause as much trouble for security as it's meant to solve.

The case of PredPol

Sophos CTO Joe Levy said he's been thinking hard about the topic ever since reading Evgeny Morozov's "To Save Everything, Click Here" a few years ago.

In that book, Morozov describes the crime prognostication system known as PredPol and the problems some see in how it calculates where and when crime will occur using algorithm software similar to what Facebook and Amazon use to fashion ads to individuals.

Privacy advocates have raised concern that the information used to build the algorithms is biased against minorities.

A Washington Post article last year painted a picture of those privacy concerns:

"Some police departments have hailed PredPol and other systems as instrumental in reducing crime, focusing scarce resources on trouble spots and individuals and replacing officers' hunches and potential biases with hard data. But privacy and racial justice groups say there is little evidence the technologies work and note the formulas powering the systems are largely a secret. They are concerned the practice could unfairly concentrate enforcement in communities of color by relying on racially skewed policing data. And they worry that officers who expect a theft or burglary is about to happen may be more likely to treat the people they encounter as potential criminals."

In that excerpt, we see both sides of the argument around GDPR's Right of Explanation provision.

On one side, the right to explanation is about protecting privacy. On the other side, it's about a regulation messing with machine learning systems that are proving effective in building better security and crime-prevention programs.

Rewrite GDPR provision or play a longer game?

It's reasonable to argue that some algorithms collect data that can violate a person's privacy while having no impact on the problems they were originally set up to solve.

It may even be reasonable to suggest the GDPR right to explanation provision be rewritten. One area where it could offer greater consideration is in providing better intellectual property protections to the inventors of the algorithms, Levy noted.

But it's also fair for someone to say GDPR isn't the problem, or even the algorithms for that matter. Rather, the problem is in the humans who set the algorithms. Shouldn't the fix be happening there, during the development process?

Cathy O'Neil is a former Wall Street worker who quit after the last economic crash, joined the Occupy Wall Street movement and now publishes the mathbabe blog. She suggested the answer is yes in her book "Weapons of Math Destruction." A Wall Street Journal article on the book sums up the essence with this headline: "Algorithms Aren't Biased, But the People Who Write Them May Be."

In our own image

Levy believes we're on path to a future where asking an algorithm why it reached a certain conclusion will be much like asking people about their judgments or tastes. The answer might resemble "just because" as algorithms become more like the minds that create them.

"As we entrust algorithms to produce more complex classifications and predictions, we'll be asking them to venture out of the light of objective truths into the shadows of subjectivity," Levy said. "Questions are bound to arise about the 'fairness' of the training sets, about the social and political leanings of the company that produced the algorithms, and whether any of the values of individual programmers had any influence."

As we allow them to learn in the wild (rather than in controlled development environments), we'll need to worry about them being corrupted by mischievous or malicious actors.

"It begins to sound a lot like raising kids," Levy said.

O'Neil says one long-term fix is to create more transparency. For example, she wrote, consumers should get an alert whenever their information is used on mathematical profiles. Consumers deserve to understand how scores like those used by car insurers are calculated. If the information used to create such scores is wrong, she wrote, people deserve an opportunity to flag and fix it. Of course, this would create new costs to businesses using and creating algorithms as they will have to separate real disputes from fraudulent disputes. But, Levy noted with a smile, "There are sure to be algorithms that could help with that."

Analysts Bryce Goodman and Seth Flaxman wrote in their paper, "European Union regulations on algorithmic decision-making and a right to explanation," that despite the problems right to explanation presents, there are also opportunities to make better algorithms. They optimistically wrote:

"While this law will pose large challenges for industry, it highlights opportunities for computer scientists to take the lead in designing algorithms and evaluation frameworks which avoid discrimination and enable explanation."

Since we're still a year away from GDPR taking effect, it'll be some time before people on either side of the data-collecting argument get to see if they are right or wrong in their current concerns.

In the meantime, we should all continue to keep working to ensure they collect information in the fairest, most accurate way possible.

EU General Data Protection Regulation (GDPR) – Reference Card

The EU GDPR will be enforced from 25 May 2018, and it is the culmination of years of work by the EU to reform Data Protection regulation into a Union-wide framework instead of a patchwork of country-specific legislations. The GDPR affects all organizations that hold personal data on EU citizens, regardless of where the organization is based in the world. The maximum fines for non-compliance are the higher of €20m and 4% of the organization's worldwide turnover.

REQUIREMENT	SOPHOS PRODUCT	HOW IT HELPS MEET COMPLIANCE
Stop the top causes of data loss		
Stop malware and ransomware	Intercept X	Keeps your endpoints secure from the latest malware and ransomware.
Keep your data secure if devices are lost or stolen	Sophos Central Device Encryption	The easiest way to manage full disk encryption on PCs and Macs that secures your devices so data on the disk is always safe even if lost or stolen.
	Sophos Mobile	Protects data on mobile devices and includes comprehensive anti-theft and loss prevention.
Stop threats at network perimeter		
Stop data-stealing attacks at your network perimeter	XG Firewall	Synchronized Security working with endpoint protection to automatically identify and isolate compromised systems.
Automatically encrypt or block sensitive data in emails	Secure Email Appliance Gateway	Automatically blocks malicious emails and encrypts sensitive email attachments.

EU General Data Protection Regulation (GDPR) – Reference Card

REQUIREMENT	SOPHOS PRODUCT	HOW IT HELPS MEET COMPLIANCE
Stop human error		
Keep individual files secure wherever they go	SafeGuard Encryption	Next-gen file encryption keeps your data safe even when it leaves your corporate network and devices.
Protect sensitive data in the cloud	SafeGuard Encryption	Automatically and seamlessly encrypt and decrypt files as they are uploaded or downloaded from public cloud storage services like Dropbox and OneDrive.
Prevent unintentional disclosure	SafeGuard Encryption	Synchronized Encryption that is always on makes sure all files are always encrypted everywhere.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK