Do Privacy and Data Protection Regulations Create as Many Problems as They Solve?

Divergent goals often result in data protection laws that are fundamentally flawed

By

Kevin Townsend

June 21, 2022

Divergent goals often result in data protection laws that are fundamentally flawed

Privacy and data protection regulations can be viewed as just another cybersecurity threat. The risk delivered is financial loss (through imposed fines) and reputational damage (caused by the inevitable conclusion that the company doesn't care about its users). Regulatory compliance should therefore be the subject of a risk management approach.

The problem

The primary problem is that there are so many different regulations. They exist at international, state and industry level, and are not always entirely consistent. And they all have fundamental weaknesses in design.

The first weakness is that they are often populist in origin, but economic in application – and these two forces often act against each other. The second is that regulators cannot keep pace with technology. And a third is that regulators are not security practitioners and don't necessarily understand the application of cybersecurity in practice.

GDPR provides a good example of the first weakness. It was designed by the elected members of the European Parliament, largely as a populist reaction to the Snowden leaks about NSA and GCHQ surveillance. However, oversight comes from the unelected European Commission, which has little direct connection to the people and a stronger responsibility for the EU economy.

The European people want their personal data protected from 'abuse' from intelligence agencies such as the NSA and GCHQ, while the Commission wants the free flow of data between the EU and US for purely economic reasons. This conflict of interest has led to an impasse that has existed from the day GDPR became law – and is not yet resolved.

The basic issue is that **US FISA 720** rules give the US government access to European PII held by US firms – which is simply unacceptable to the letter of the people's GDPR. The EC's first attempt to overcome this issue, the Safe Harbor agreement that allowed transatlantic data flows, was struck down by the European Court as unconstitutional. Its successor, Privacy Shield, suffered the same fate for the same reasons in what is known as the Schrems II ruling.

Now the two sides have reached an agreement in principle for a third 'safe harbor' arrangement – but the details are not yet known. All that has been announced are vague words like those from the White House: "The United States has committed to implement new safeguards to ensure that signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives…"

Most European observers doubt that this will be sufficient to satisfy the letter of the law contained within GDPR, leaving the strong likelihood that the new transatlantic data privacy framework will also be struck down by the European Court.

The apparently irreconcilable conflict between populist preferences and economic necessity will continue to undermine the very credibility of GDPR. The result, as Dave Johnson, CEO and founder of Rixon, comments, "You're basically throwing darts in a dark, blacked out room hoping you're going to hit the targets. It's hard, it's really hard." In simple terms, regulations create as many problems as they solve.

Sounil Yu, CISO at JupiterOne, highlights another conflict of interest within regulation design. "Many of the US local laws are contradictory and that is no surprise since governments are trying to address two seemingly irreconcilable objectives: protecting security and privacy while trying to enable access for law enforcement, espionage, and surveillance. These two divergent goals often result in data protection laws that are fundamentally flawed."

Even beyond such problems, many security leaders believe that the strictures of data protection regulations can divert energy and budget away from what is really required for cybersecurity. Compliance is not security, they say – often falling back on the hope that security is compliance. This approach hopes that being secure will lead to automatic compliance – a belief that may not always be adequate.

"Regulations are both good and bad," comments Laura Whitt-Winyard, CISO at Malwarebytes. They are good for those companies who don't take security seriously – regulations at the very least force them to check the boxes. They are bad when they give companies a false sense of security, thinking that if I have checked all the boxes then I must be secure. We all know that is inaccurate as evidenced by the multitude of 'compliant' companies that have been breached."

The value of regulations

The hope that security will provide compliance relies on two basics: the demonstration of good security practices and the luck of not being breached. With proof of serious cybersecurity best practices and controls, most regulators will at least reduce the severity of any fines imposed for non-compliance. The best way to achieve this is to be able to demonstrate conformance with at least one of the top cybersecurity frameworks – such as the NIST Cybersecurity Framework bolstered by Cybersecurity Supply Chain Risk Management (SP 800-161), and/or ISO 27001.

Whether this is enough is a moot point – these publications are frameworks rather than regulations. The overall value of regulations is also moot. "They're like medicine," comments Martin Zinaich, CISO at the City of Tampa; "good in the right doses." Left unsaid is the reality that medicines often have unfortunate side effects.

Zinaich believes PCI is an example of a good regulation, but notes that it can be reduced to a meaningless tick box exercise if companies choose to self-audit. "What it does do," he continued, "is provide the practitioner with a toolbox for personal use, or to take to the board, saying, 'We need to do this, but we're way under compliance levels'."

The same can be said for some other regulations in some instances, but Zinaich adds, "The piecemealing of regulations isn't going to be good. We're going to get policies based on the threat du jour that won't apply a holistic view of cybersecurity." Trying to piecemeal security will leave inevitable gaps. And there is a very common perception that regulations are simply focusing bureaucratic vision on the most recent lightning bolt, after it has struck.

Here it is worth considering the value of Executive Orders (EOs). These can be viewed as regulations for federal agencies, and advice for private industry – and the Biden May 2021 EO titled *Executive Order on Improving the Nation's Cybersecurity* is a good example. The standout features of this EO are increased focus on zero trust and improved supply chain security. But supply chain attacks have been increasing for years and security leaders have long been focused on zero trust. It is effectively yet another 'regulation' that is chasing lightning and filling holes rather than providing a holistic preemptive approach to cybersecurity.

Plotting a path through the regulations

"Keeping up with the various state, local, and international privacy laws and regulations requires a concerted effort and focused strategy," suggests Rick Holland, CISO at Digital Shadows. "CISOs must have their Governance, Risk, Compliance (GRC), and Privacy teams engage with peers, regulators, and outside counsel to stay up to date."

It also benefits if these teams actively participate in groups such as the International Association of Privacy Professionals (IAPP) and the Information Systems Audit and Control Association (ISACA) to keep up with the trends.

"The good news," he continued, "is that GRC software enables you to track all your compliance and regulatory requirements (such as GDPR, SOC 2 Type 2, ISO 27001) in one platform and crosswalk them to create a matrix of controls that will meet all your obligations. This matrix makes it much easier to map and implement the various controls to ensure you address them."

The need for teamwork in navigating the sea of regulations is supported by Yu. “We can’t expect one person to be cognizant of all the relevant local laws,” he says, “so it is important that the CISO work as a team with other regional and sector-specific information security experts that can ensure that we remain compliant.”

“I always recommend going with the most stringent,” says Whitt-Winyard. “If you are doing security the right way, you will be compliant. Security equals compliance, not the other way around.”

Solutions

In the US, there can be no solution to the regulations dilemma without an overarching federal law that overrides multiple, potentially conflicting, state laws. GDPR was Europe’s solution to the same problem. Europe had multiple approaches to data and privacy legislation across its different member states. The solution, eventually, was a single regulation across all members. But it took many years and much compromise to achieve – and the result is complex and unwieldy.

The US currently has similar issues, but across states rather than nations. It is made more difficult by the existing extremely partisan nature of US politics. Any federal law proposed by a Democratic administration is likely to be resisted by Republican states – and vice versa. It’s not impossible, however, because ultimately privacy is a people issue rather than a political issue. Nevertheless, it would require bipartisan approval for its development to survive any possible administration change during its development.

Whether it will ever happen is unclear. Many practitioners believe it *will* happen simply because it *must* happen. Others believe the difficulties are too extreme, and it won’t happen. However, if a strong federal privacy and data protection law came into force, it could potentially also solve the transatlantic data flow problem. If the EU were to recognize the US as having equivalent privacy controls, there would be no need for a separate ‘privacy shield’ agreement.

The only alternative to federal regulation would be to regulate the security practitioners across the whole country rather than the security controls within individual companies. This could provide a vehicle for trans-state conformity to a professionalism set by an independent professional body. There has been some interest in this among cybersecurity leaders, but little movement towards it.

The question now is whether it is too late for practitioners to regulate themselves from within, leaving only the option of the government imposing regulation from above. Longstanding proponent of self-professionalization, Zinaich, commented, “I almost feel like it is too late for self-professionalization.”

Patrick Forbes, CISO at S&P Global, disagrees. “It is not too late,” he said. ‘Companies and the industry are very eager to have improved guidance and evolve beyond NIST CSF or ISO 27000 with a globally recognized maturity standard. Company boards are constantly asking for how their company stacks up against a standard or their peers. At the moment, the industry is still waiting for and eager to use a ‘go-to’ standard similar to NIST CSF that also measures maturity.” It is effectively the same argument as that for a federal privacy and data protection law.

Whitt-Winyard feels it is not only too late for self-professionalization, but wrong in principle. “Yes [it is too late], she said. “The sheer dynamic nature of cybersecurity makes the ability to come up with a baseline near impossible, and the field is too broad to professionalize.”

She continued, “The cybersecurity community is built of those who learned this field in their own time, on the fly during an incident, as teenagers or interns and so on. These people have an insatiable urge to learn and explore. They are filled with passion and persistence, can think like the bad guy and have an unwavering curiosity. These are traits that you cannot teach at university. If cybersecurity became professionalized, it would create additional barriers for those entering the field – and we have had a shortage of skilled cybersecurity talent for as long as I can remember.”

The implication is that regulating the people rather than the posture will have an overall negative effect on the cybersecurity of the nation. But at the same time, standardized privacy and data protection industry regulations across the whole of the US are a long way off, even though sorely needed. The industry and government, minus lobbyists, need to come together from the bottom up rather than top down – and talk about regulations.