ARI 97/2019
14 October 2019

Cyber Security: How GDPR is already impacting the public-private relationship

Danny Steed | Head of Strategy, ReSolve Cyber | @TheSteed86

Theme

For anybody wanting to participate in a public-private relationship within the General Data Protection Regulation (GDPR), the calculus must be weight of the well-known "carrot" gained from collaborative exchange with the new regulatory "stick" being wielded in Europe.

Summary

The public-private relationship has long been heralded as a key arena in cyber security, where collaborative arrangements can ensure greater resilience to cyberattacks and swifter responses to cyber incidents. This article argues, however, that the relationship will change greatly in a post-GDPR world. The relationship should now be considered as one where collaboration is augmented with coercive measures in order to change private sector behavior in cyberspace.

Analysis

The arenas, industries, and actors that cyber security affects are today almost too vast to fully cover. Cyberspace has become ubiquitous throughout our economies, infrastructures, and our individual lives, so cyber security too is therefore ubiquitous. Regardless of whether one is addressing cybercrime amongst civil society, to organized cybercrime against corporate enterprise, or through to state level cyberattacks and espionage between nations, cyber security has become a central concern to all in both industry and government.

Within this concern it has long been believed that a key remedy in ensuring better cyber security throughout society has been to cultivate an enduring public-private relationship between the state and the core components of its economy. The motivating logic being that, with a culture of information sharing at its heart, contributions to policy discussions and greater awareness of each other's positions, greater resilience and behavior could be established to reduce the impact of cybercrime throughout nations' respective economies.

While there have been measures of success, it cannot be claimed that other factors have not impacted consideration as to how else cyber security should be managed, which in the EU has led to the implementation of the General Data Protection Regulation (GDPR) in 2018. Following scandals such as Cambridge Analytica and Facebook in recent years, as well as a veritable catalogue of increasingly severe data breaches, concerns about the use and misuse of data have evolved into what *Wired* has imaginatively –although

certainly accurately– termed the "Great Privacy Awakening".[1] It has since become clear that the maturing approach to addressing cyber security lies as much with coercive regulatory measures as it does with collaborative public-private relationships. Simply put, big tech cannot be trusted to regulate itself.

What this article argues, however, is that measures such as GDPR are sure to impact the fruitfulness of any public-private relationships moving forward, with very notable cases already illustrating the changed dynamic that is certain to become the norm. Any consideration of the future of the public-private relationship within and among EU nations must also now strongly factor in the impact of GDPR, particularly as a deterrent to private sector organizations, from giving more to national level cyber security resilience. At its core, for anybody wanting to participate in a public-private relationship within GDPR's jurisdiction, the calculus must be weight of the well-known "carrot" gained from collaborative exchange with the new regulatory "stick" being wielded in Europe.

The public-private relationship: What and Why?

Public-private relationships have experienced many manifestations across numerous nations, of course predating cyber security concerns as well. Definitions can prove troublesome due the catalogue of varied approaches and recommendations and are perhaps not the best place to begin in understanding what they are. Instead, it is better to understand why they are necessary in the first place. Christensen and Peterson were correct when they highlighted then President Obama's opinion of the cyber challenges, that "This is a shared mission" that must include private sector input every bit as much as the public sector.[2]

The key need for such a relationship lies in the recognition that certain national and societal challenges extend far beyond the capability of the state alone to tackle, that private sector bodies are key stakeholders, and that a sense of shared responsibility is recognized. Cyber security certainly qualifies for this measure, with the three key aspects of a public-private relationship –risk sharing, innovation, and longevity– a clear necessity in finding long-term solutions to cyber security issues.

Despite this, clear ideas as to what the public-private relationship is for cyber security has, according to Madeline Carr, "always been unclear".[3] This is because, fundamentally, there remain challenges between what the public sector and private sector seeks to achieve through the relationship at its core. The public sector approaches public-private relationships with national security objectives in mind, whereas the private sector engages in order to pursue market-based objectives at minimizing liabilities in the market. It is on this basis that readers must always recognize that achieving and

[1] Issie Lapowski (2019): 'How Cambridge Analytica Sparked the Great Privacy Awakening', *Wired*, 17/IX/2019, https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/.
[2] President Obama quoted in Kristoffer Kjærgaard Christensen,and Karen Lund Peterson (2017): 'Public-private relationships on cyber security: a practice of loyalty', *International Affairs* 93:6, p. 1437 and 1439, https://academic.oup.com/ia/article/93/6/1435/4568587.
[3] Madeline Carr (2016): 'Public-private relationships in national cyber-security strategies', *International Affairs*, 92:1, p. 61, https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf.

maintaining any public-private relationship is a fragile affair, with numerous actors pursuing a variety of different, if not always opposing, objectives.

Key cases in GDPR to date

The implementation of the General Data Protection Regulation Act across Europe since May 2018 has already had immediate impact in the cyber security landscape, not only for Europe but worldwide as well. A clear example of the concerns raised could be seen from numerous American publications –particularly the publishing houses of major news outlets–[4] who replaced their homepages for European readers with a landing page announcing, in effect, a denial of service until the ramifications of publishing into the jurisdiction of GDPR have been clarified.

The private sector immediately became concerned about walking into regulatory fines on a scale not seen before. This is understandably so, with the fines set to be faced now ranging to 4% of total turnover or €20 million, with the emphasis being on issuing a fine for the highest amount of the two. To put this into context, although domestic fines varied across the continent under the previous legislation, for one example under the UK's previous Data Protection Act the maximum fine faced by organizations was £500,000. This maximum fine was only ever issued once, against Facebook in October 2018 following the Cambridge Analytica scandal.[5]

Following the implementation of GDPR, it has been a question of wait and see who would become the first victims of the new regulatory big "stick" on the European continent. In 2019 we now have two key cases to explore the impact of GDPR on the public-private relationship, British Airways and the Marriott International hotel group.

Anatomy of a hack: British Airways and Marriott International

In September 2018, the personal and financial information of an estimated 380,000 British Airways passengers was compromised. Between 22:58 (British Summer Time, BST) on 21 August and 21:45 (BST) on 5 September 2018 a malicious piece of software –22 lines of code linked to the British Airways baggage claim information page– harvested the payment details of passengers purchasing tickets from the British Airways portal, including card verification value (CVV) numbers. The software script ran with the intent to capture payment details at the point of payment, thereby not breaching British Airways servers but instead stealing payment information at the point of interaction between payment and airline databases.[6] This form of attack, commonly known as *formjacking*, avoids the difficulty of breaching databases and servers directly, focusing instead on targeting the exchange of monies.

[4] Renae Reints (2018), 'These Majors U.S. News Sites are blocked in the EU', *Fortune*, 9/VIII/2018, https://fortune.com/2018/08/09/news-sites-blocked-gdpr/.
[5] Information Commissioner's Office (2019): 'ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information', ICO, United Kingdom, https://ico.org.uk/facebook-fine-20181025.
[6] Jordan Bishop (2018): 'This is how 380,000 British Airways Passengers Got Hacked', *Forbes* (11/IX/2018); Lily Hay Newman (2018): 'How Hackers Slipped by British Airways Defenses', *Wired*, 11/IX/2018.

Meanwhile, Marriott International suffered a data breach in 2018, following the discovery and tracking of a Remote Access Trojan (RAT) active on Marriott's Starwood's IT network from September through to clear knowledge of an active breach in November 2018. Once the key discovery in November was made that the RAT has been present on the network since 2014 –prior to Marriott's acquisition of Starwood– it was clear that there was indeed a bad problem.

Marriott issued a public notification on 30 November of a data breach, with an estimated 500,000,000 customers affected. Within these enormous numbers were included 5.25 million unencrypted passport numbers and 385,000 payment card numbers that were still valid at the time of the breach.[7] Unlike the British Airways hack targeting financial exchange, Marriott's experience highlights the risks associated with due diligence when carrying out a corporate acquisition.

Under the authority of GDPR, the British Information Commissioner's Office (ICO) chose to impose a fine of £183 million on British Airways. This was levied at 1.5% of the airline's 2017 turnover,[8] revealing both a significant watermark beyond previous maximum regulatory fines while also still remaining significantly below GDPR's 4% maximum cap. Continuing to send a loud message globally, the ICO was quick to follow up its BA fine with a fine of £99 million levied against Marriott. The filing specifically citing that Marriott "failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems".[9]

The impact on the public-private relationship

At this stage, one might question the impact of GDPR on the public-private relationship and consider them to be two separate issues entirely. This is certainly not the case, with the argument presented that the new practice of fines being implemented against the private sector represents the first step of difficulty to affect the public-private relationship moving forward. This impact will evolve in four ways; a divergence of interests, increased uncertainty in trust, greater fear of regulatory punishment, and an increased difficulty to entice private sector collaboration.

In the first instance, an already fragile balance of interests will continue to diverge. Now that the public-private relationship is no longer one born of purely a rewarding "carrot" but also a punitive "stick", the private sector now knows that the public sector will seek to punish misdeeds against the data they bear the responsibility to safeguard. This dynamic can only serve to increase the distance between interests that were always difficult to align and maintain in the first place, the pursuit of generally national security interests on the part of the public sector, and the pursuit of market stability and competitiveness on the part of the private sector. A careful balance must be achieved if any functioning public-private relationships –especially in the realm of information sharing– is to endure.

[7] Catalin Cimpanu (2019): 'Marriott's CEO shares post-mortem on last year's hack', ZDNet, 3/VIII/2019.
[8] C.R. (2019): 'British Airways faces a £183m fine over a data breach', *The* Economist, 7/VIII/2019.
[9] ICO quoted in Zack Whittaker (2019): 'Marriott to face $123 million fine by UK authorities over data breach', *Tech Crunch*, 7/IX/2019.

This brings us to the second dynamic, a greater uncertainty in the bedrock of the relationship –trust. The key dynamic that underwrites the public-private relationship is trust between the actors involved. With regards to information sharing, trust in the discretion exercised in disclosure not being made outside of the trusted circle is paramount. An increased punitive framework decreases the incentive to share information as fully as could be expected otherwise.

The third impact is that a greater fear of regulatory punishment logically increases the fear held by any private sector body in the relationship, only exacerbating the issue of trust placed in the public sector. A question would be posed by any business facing this, which is "how can a private sector body trust public bodies to help in hours of need when a firm may well be opening itself up to a punitive regulatory measure?"

Finally, if these first three dynamics only increase, there will be an increased difficulty in enticing existing outsiders to join a public-private relationship for cyber security. Why would new private sector bodies join a relationship if the dynamic with existing members has visibly shifted from one of collaborative exchange to one of potentially large regulatory punishments? Given the reaction of many American news outlets in blocking webpages to European visitors in 2018, it is entirely plausible in the American example to believe that their businesses would be hesitant to participate in European public-private relationships with such a question hanging over their decision making.

These dynamics are clear and present in the maintenance of a healthy public-private relationship. Such a relationship that is geared towards cyber security is fundamentally built around information sharing as its core manifestation, initiatives like the FS-ISAC grouping for the financial sector[10] in general and the UK Government's Cyber Information Sharing Partnership (CiSP) [11] platform in particular being exemplars of long-term relationships in practice.

How to maintain public-private relationships post-GDPR

So far, readers might infer that the GDPR holds a purely negative effect on the public-private relationship. While the argument here is certainly that the dynamic has changed considerably, it is still seen as being fully within the ability of relationship managers to balance effectively. Public-private relationships focused on cyber security certainly have a healthy future in a GDPR world, which when manifested in information sharing practices are always overwhelmingly focused on achieving two objectives: the prevention of cyber security incidents through building increased resilience, and the mitigation of actual incidents through the sharing of essential information to reduce harm.

Those core objectives are not incompatible with GDPR but do require careful management from the public sector in order to not be seen by private sector bodies as

[10] The Financial Services Information Sharing and Analysis Centre (https://www.fsisac.com/), although a private initiative, shares common public-private relationship goals and is a well-known example of an information sharing initiative.
[11] The Cyber Information Sharing Partnership (https://www.ncsc.gov.uk/section/keep-up-to-date/cisp) began in 2014 under CERT-UK before being transferred to the National Cyber Security Centre (NCSC) upon its formation in 2016.

no longer worth their investment if the regulatory punishment outweighs the collaborative gains. Two guiding principles can serve to assist this relationship moving forward.

Establish clear boundaries

There are numerous factors that serve to build public-private relationships, with plenty of views on offer from many researchers. Almost all, however, begin with a clear recognition of the foundational factor, trust.[12] In any public-private relationship, the place of trust is paramount in bringing and keeping stakeholders at the table; no practice of information sharing to prevent and mitigate cyber security incidents can take place if the participants do not trust that sensitive information is handled discreetly.

The establishment of clear boundaries is therefore essential. In particular, to make sure than the forum for the exchange of information is protected from regulatory involvement. There can be no faithful exchange of sensitive information if a relationship carries the fear that regulators are also present. In as far as it is possible to achieve within each European nation's domestic legal environment, the public-private relationship for cyber security should be separated from the activities of the regulatory bodies charged with pursuing GDPR cases.

Should there be any doubt in the logic of this position, the justification can be made immediately apparent. Even in a "carrot and stick" relationship, the presence of the stick does not remove the "carrot" outright. The place for incentives remains even in the presence of punishment. So too with GDPR, the presence of regulatory fines does not remove the clear and present need for an incentivizing relationship that seeks to prevent harmful cyber security incidents in the first place. Indeed, to fall back on a position of claiming that GDPR could solve cyber security itself would be to accept a position of accepting an increase in incidents and simply to punish victims after the act. Such a position is not only illogical, it is plainly against the public good even when referring to private actors.

Advise, don't mandate

Building on the first principle of establishing clear boundaries is another principle for the public sector, which is to advise, not mandate the actions of private actors within their public-private relationship. The central dynamic of such a relationship is the *mutual* exchange of information for *mutual* benefit. If the public-sector hosts of the relationship believe their role is to mandate, the balance of the relationship will be put under the impression of a hierarchical one.

This is particularly acute when it comes to the submission of live incident information. Public actors are frequently sought for guidance on incident response and mitigation measures, as well as advise on what steps to take from a law enforcement angle. The

[12] Many views are on offer, but the following will endow readers with the core case behind trust.
Max Manley (2015): 'Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Relationship', *Journal of Strategic Security*, Vol. 8, No. 3, p. 98; and Eric A. Kaijankowski (2015): *Cybersecurity Information Sharing Between Public-Private Sector Agencies,* Naval Postgraduate School Thesis, Part V: Conclusion.

boundary must be set that advice is precisely that, advice, and not an order to be followed. There must be space in a public-private relationship to hand a decision back to the private actor, the owner of the data or incident, to deliberate and reach their own judgement on what actions to take according to their legal and regulatory responsibilities.

An attempt to impose such a responsibility on those managing a public-private relationship from the public sector compromises both impartiality as well as the foundation of trust in the relationship. It is a careful, yet increasingly fragile balance to be struck in the management of such a relationship in the face of regulation such as GDPR, but one that experience in the field of public-private relationships says can be achieved.

Conclusions

To conclude, this author believes that the first year of GDPR has introduced a difficult element in the pursuit of public-private relationships for cyber security, but it is one that is within the realms of existing experience to manage. Previously, one would argue that public-private relationships were based on purely shared incentives; open collaboration and information exchange between actors to prevent and/or mitigate cyber security incidents. To this “carrot” has however now been added the “stick” of GDPR, which is a recognition that public-private relationships by themselves have not been enough to condition both the cyber security landscape and the behavior of actors within it as desired.

While it cannot be argued that there is a need for increased regulatory punishment to match the scale of misdeeds that have evolved in the handling of data and incidents, it must also recognized that GDPR introduces an element of doubt in the minds of those who may be hesitant to contribute to public-private relationships. Those charged with maintaining and growing these relationships in the pursuit of greater resilience to the cyber threats faced need to work to ensure that the new regulatory “stick” is not seen to overshadow the many benefits that come from the “carrot” of mutual information exchange. A world in which cyber security is managed only by the issuing of punitive fines would become a sad place indeed.