ONE YEAR OF THE GDPR: HEIGHTENED ENFORCEMENT

By George S. Takach

Regular readers of this space will know that in Europe a new General Data Protection Regulation ("GDPR") came into force all around the European Union in May, 2018. It contains many new provisions, and some eye-popping numbers for maximum fines (i.e., 4% of global sales of the offending business). So, a year later, what can we say about how the law is being administered, and, perhaps most importantly, what has been its impact on corporate and other behavior in the increasingly important online and digital privacy space ?

These questions are obviously important if you're a Canadian company or other organization with operations in Europe, or you collect data from Europeans on a regular basis (ie – you run a website that regularly caters to a world wide audience, but you also target ads and other internet outreach to Europeans). But in addition, even if you do not have meaningful or sustained connections with Europe, you should still follow developments in respect of the GDPR because clearly it is emblematic of the wave of the future when it comes to privacy regulation in the online and digital spheres. And as I mentioned in a recent column in this space, Canada looks to be set to be gearing up for significant changes in its own data protection laws and regulations, so in the not too distant future what you are about to read below will be very directly applicable to you – so you may want to join many other businesses and organizations that are improving their privacy practices now to new best practice levels even before the legislation is passed requiring them to do so.

Heightened Enforcement

The big story for the first year of GDPR has to the heightened enforcement – this is the headline. And the numbers are getting bigger and bigger, and certainly bigger than they were under the previous legislation. A major airline was fined the equivalent of $302 million in respect of a data breach, after they were found by the privacy regulator to have lax cyber security. This is a very muscular decision, and it does not surprise me at all that it came out of the cyber security environment. The reason I say this is because when my colleagues and I are negotiating large technology procurement transactions, such as major outsourcing deals, particularly for SaaS-based services, the cyber security provisions of the contract are by far the most heavily negotiated today (far more contentious, for example, than the intellectual property indemnity clause); and in respect of the limit of liability clause, it's intersection with cyber security is also heavily contested, as both sides bring an extremely augmented sensitivity to the topic.

Another large enforcement action arising out of a data breach involved a hotel chain; in this case the fine was $162 million. What was very interesting about this case was that the target of the proceeding, and the direct subject of the fine, was the purchaser of the problematic, insufficiently secure data infrastructure, which they had acquired in an M&A deal some time before. But did the regulator give them a pass – absolutely not ! If you are in corporate development, you really need to take note of this case. From the perspective of cybersecurity, how are you doing in your acquisition deals on the due diligence front with respect to the target's computer systems and data handling practices ? Particularly if they have a B2C business that collects, processes and stores large volumes of personal information, a cursory review and a few questions of their IT department don't cut it any more. You really have to get some technical experts into the target's data centre, and review for vulnerabilities. And if you find some, it's not the end of the world…..so long as you make it a priority to shore up the

systems as soon as you close the deal. Don`t wait, don't prevaricate. Act right away, and bring those systems you are now accountable for at least up to the standards you have in your facilities. And yes, you either have to build that extra expense into your financial model for the deal; or you have to try to negotiate an adjustment to the purchase price, because likely the sellers under invested in cyber security for years, from the sound of it. But in any event, you have to find a way to pay for the rectification of the required digital security deficiencies.

What's interesting about these two enforcement cases is that neither involved a big American tech company; rather, they were traditional businesses. Now, of course (and I`ve been saying this for some time), today every business is a tech business. And so if you think "our core business isn`t selling internet-based services, so I really don`t have to take cyber security too seriously".....well, you would be wrong. If you collect any personal information from customers, you have to be right in the thick of worrying about cyber risk, and how to mitigate it through techilogical and other best practices – there is simply no way around it anymore. This is the prime lesson to be learned from the first year of the new European data protection law.

More Accountability from Internet B2C Businesses

While digital privacy is today every organization's business, of course that is doubly true of companies that make the bulk of their earnings from online services for consumers. And sure enough, the third largest fine last year under the new EU privacy regime for a data protection shortcoming was to Google, for $73 million. The offence was, put simply, for offering only one option for consent to online targeted ads. This raises another aspect of the GDPR – namely the European privacy regulators are working hard to breathe new life into the concept of consent. This is very telling, because for us, in Canada, the concept of consent has been at the very core of our data privacy law (PIPEDA), and the various provincial equivalents, right from the beginning (going back some 20 years now).

For example, there are also new GDPR rules on getting consent for cookies, perhaps the most common request on websites today. In a nutshell, the European legal requirements require the website operator to provide greater transparency into the operation of the cookie, and meaningful choice in acceptance (ie – it helps to give a decline button). There is however, also a new exemption if the website has an existing relationship with the consumer and the data is processed in a manner that is reasonably expected. In a nutshell, consent continues to be a very contentious topic in privacy circles, and if you are responsible for your organization's web presence, you have to stay on top of all these developments.

Beyond consent, the big American tech companies are also getting pulled over to the side of the digital highway (bet you haven`t heard that phrase in a while….:) by the regulators for a range of alleged infractions in Europe, including Microsoft and Apple. But what many don`t realize, is that a very large number of smaller players are hearing from the regulators as well, and in many cases fines in the $ 15,000 - $ 50,000 range are also being levied (about 90 smaller companies were fined a collective $8.7 million last year. So, you should disabuse yourself of the thought that privacy regulation is only a concern for "Big Tech"; that was never a responsible attitude, and now the enforcement patterns of the European data protection regulators are proving that beyond any shadow of a doubt.

Raising Awareness

A few years back, a number of pundits in the media predicted that privacy was dead, that people were no longer interested in their privacy rights, and everyone should just get over these

twin facts of life. The GDPR, and the raised awareness level that it has ushered in, has put the lie to this sentiment. A recent poll found that fully 73 % of Europeans (a huge portion, in my view) knew of at least one specific right in the GDPR. So, it does not come as a surprise to me that last year fully 89,000 data breach incidents were reported to the privacy authorities. That number is twice what it was the year before….twice ! In a similar vein, some 144,000 privacy complaints were lodged with the regulators in the first 12 months following the coming into force of the GDPR. Again, I think that is a huge number, keeping in mind that privacy compliance is not that big a thing in the eastern countries of the European Union; so, we're seeing an exceptional rate of awareness of privacy questions in the Western European states, especially the UK, France, Germany and Spain.

The other thing to remember about GDPR compliance is that it's not just about fines, while certainly they grab all the headlines. It's also very much about orders issued to cause the cessation of data processing; or the order requires some corrective action. These sorts of remedies that can be foisted on companies under GDPR can be even more difficult for companies to comply with than payment of a simple fine. So, ultimately it comes as no surprise to me that, since the time GDPR came into force (May, 2018), over 500,000 organizations have dutifully registered their data protection officers. And these persons are being given increased powers to help ensure that their organization doesn`t fall afoul of the new privacy law regime.

What makes all of this quite astounding (are you sitting down ?), is that all this compliance activity noted above may in fact be just a preview of what's to come, and frankly not a very indicative one at that. I say this because the first year of GDPR was always intended to be something like a "burn in period"; a fairly low level of regulatory activity to give business and citizens (who increasingly are actively bringing cases directly against the corporate behemoths) a period of time to adjust to the new rules. If this is indeed the cadence, it will be very interesting to see what the enforcement "year in review" looks like next year!