Making GDPR compliance a competitive advantage

Alvin Cheung, runner-up in *PL&B's* student essay competition 2019 discusses why competitive advantage is hard to achieve through privacy.

Theoretically, GDPR[1] compliance should bring competitive advantage. One only needs to go back to early 2018 when it was revealed that Cambridge Analytica harvested the personal data of millions of people's Facebook profiles for political engineering, precipitating an incredible fall in Facebook's stock price which was indicative of the loss of public confidence in the platform. From that episode, it was clear that people valued privacy. The introduction of the GDPR seemed to be the perfect opportunity for companies to differentiate themselves from market competitors, based on faithful adherence to the Regulation and a commitment to protecting data subjects' rights.

Companies should see GDPR-compliance as a competitive advantage in the same way companies saw big data analytics as a competitive advantage a decade ago. Similarly, both respond to customers' wants: now it is privacy, then it was that of convenience and personalization in web-related products. Corporations adopted business models and strategies which rely on personal data as a key input to create competitive advantages: including the imposition of multi-sided platforms by data-driven mergers (Microsoft/Yahoo! Joint venture, Facebook/Whatsapp merger).[2] Yet, even though 93% of companies in the EU and US expect to be GDPR-compliant by the end of 2019 – which shows the inherent value of becoming privacy law compliant – only 50% of the companies believe that GDPR-compliance allows for a competitive advantage.[3] Why is that? If companies are not convinced that GDPR-compliance is a competitive advantage, what is the compelling case for realistically "making" privacy law compliance a competitive advantage?

This essay will attempt to do three things: first, examine how companies can theoretically secure a competitive advantage by becoming privacy law compliant; second, argue that market realities do not convince companies that GDPR-compliance allows for a competitive advantage; third, argue that legal questions pose significant problems in convincing certain industries that GDPR-compliance creates a competitive advantage.

Benefits of becoming GDPR-compliant

One of the main features of the GDPR is that it codified the doctrine of "privacy by design and default" in Article 25, making it a legal requirement for controllers to integrate data protection into processing activities and business practices, from the design stage to the end of the life cycle. Controllers are required to comply with this requirement by putting in place "appropriate technical and organisational measures" designed to safeguard the rights of data subjects. Of course, the GDPR seems to subtly acknowledge different firms have varying economies of scale or risk profiles, and duly advises each controller to "take into account the cost of implementation" and "the risks of varying likelihood…for rights and freedoms of natural persons posed by the processing".[4] However, one could argue that if companies choose to implement more sophisticated, "state-of-the-art" measures, such as anonymisation, pseudonymisation and encryption (Articles 6(4)(e) and 32(1)(a)), companies may well gain a competitive advantage. Indeed, pseudonymisation brings commercial benefits as well: it is easier to repurpose data; it is an expressly recognized safeguard under Article 89(1) for organisations carrying out scientific research; and it is a mechanism for removing data from the range of rights under Chapter III.[5]

If companies highlight that such technical measures are in place to protect customers' data in their privacy policies, this could breed customer loyalty too. According to a Harvard Business Review study,[6] if a company had i) explained in clear language how the company would use and share his or her customer data – including IP addresses and search histories, and ii) was providing users control over their own data with opt-out options in certain practices such as receiving promotional information from them, the effects of possible data breaches on stock prices and customer loyalty would not be so severe. Instead, "empowered customers are more willing to share information and more forgiving of data privacy breaches". Customers feel less "violated from big data practices", and were less likely to switch to alternative, competing companies. Clearly, increasing transparency and customers' perceptions of control are key: a GDPR-compliant company could sustain or improve their competitive advantage in the long-run if they highlight to customers that they have taken the most contemporary and comprehensive data protection measures.

In light of the high profile data breaches which have occurred in the past two years around the world – ranging from the Equifax breach which impacted approximately 143 million US customers,[7] to the Google+ software glitch which caused the employer and relationship statuses of 52.5 million users to be exposed,[8] it is no surprise that customers are unwilling to deal with companies known to lack adequate data protection. Recently, a study found that more than half (55%) of respondents would avoid giving data to companies they know had been selling or misusing it before.[9] The logic is that if companies could market themselves as manifesting their belief in valuing customer privacy and security by adopting the most state-of-the-art organisational and technical measures, they could gain a competitive advantage.

Moreover, data controllers are responsible for the actions taken by data processors as per Article 28(1) of the GDPR. Therefore, data processors can gain a competitive advantage by demonstrating to controllers that they exercise effective control over their data, given that high level non-compliance can lead to administrative penalties of up to 20 million, or 4% of the worldwide annual revenue of the previous financial year.[10] Therefore, an organization which can effectively demonstrate GDPR-compliance and effective control over data will be at an advantage in competing with data processors who cannot make the same claims.

Finally, companies can take advantage of the introduction of the GDPR to "take stock of its data": identifying which pieces of data are important. This will help companies leverage their data more effectively and "provide a basis for re-architecting data governance in a structure" which allows them to process customer data more effectively.[11] This, in itself, can lead to a competitive advantage.

Market realities are unconvincing

How does one gain a competitive advantage? A competitive advantage is gained by a company accumulating market power within a particular industry. If some companies are less transparent over data policies and do not comply with privacy legislation, consumers opt for compliant competitors with clearer policies that more closely align with their privacy preferences. Consumers will choose competitors who will offer them services to better protect them against exploitation, with an array of privacy-enhancing services and technologies such as encryption.[12]

However, compliance with the GDPR does not necessarily help companies accumulate market power if market power is severely concentrated in the hands of an overly dominant player. One example is that of Google: between 2011-2014, Google was accused by the Federal Trade Commission of using deceptive tactics and violating privacy promises in its proclamation of Google Buzz,[13] misrepresenting to users of Safari that it would not place "cookies" or serve targeted ads to users,[14] surreptitiously collecting huge amounts of personal information for its mapping technology Google's Street View,[15] billing consumers millions of dollars for in-app charges incurred by children without parents' consent,[16] and collecting personal data without the person's knowledge. Although Google had "committed major violations of the public trust",[17] it still retains significant market power given the monopoly it holds over the largest search engine, video platform (YouTube), one of the biggest browsers (Chrome) and biggest operating system for mobile devices (Android). Therefore, in light of the unhealthy market dominance which some conglomerates and corporate giants hold in their respective industries, smaller companies may find GDPR-compliance as utterly worthless in gaining a competitive advantage. Given the costs associated with becoming GDPR-compliant and the perceptible lack of shift in demand that would occur in a well-functioning market, it is no wonder that 50% of the companies see GDPR as an obstacle rather than an opportunity.[18] If companies do not believe that GDPR-compliance is a differentiating factor, there are two likely outcomes: first, they will continue to use violating data-driven strategies and take the risk of being found GDPR-non-compliant; second, they will complete the minimum requirement of offering basic technical and organisational measures to ensure GDPR-compliance, without viewing it as an opportunity to secure a competitive advantage.

For companies whose advertising-supported business model is based on collecting and using personal data with behavioural ads and gain a competitive advantage that way will see the introduction of the GDPR as a threat to their established competitive advantages. For example, advertising – which is tailored to each individual by processing and analysing the vast array of "detailed and specific information" - accounted for most of Facebook's revenue – 93%, 90%, and 85% in 2018, 2017 and 2016 respectively - and allowed it to reinvest in other projects such as "Stories" or platforms such as Instagram or WhatsApp to sustain its competitive advantage.[19] Thus, the legal requirement imposed by the GDPR for Facebook to use data responsibly and consensually reduces the field and spectra of data which they are able to use to create targeted ads. Thus, it harms their primary instrument of revenue-generation and profit-maximization and prevents them from enlarging existing competitive advantages.

Therefore, whilst GDPR-compliance theoretically allows companies to secure a unique, competitive market, realities seem to suggest the exact opposite.

Legal Challenges

Certain sectors are affected disproportionately. For example. an overwhelming 80% of organisations in the manufacturing sector believe that GDPR is an obstacle because they are less experienced with processes around data regulation and compliance. More importantly, legal concepts and issues surrounding the GDPR are even more alien to unfamiliarised organisations, the understanding of which will incur significant costs. Some argue the GDPR roughly retained many rights granted to data subjects[20] under the Data Protection Directive[21] – namely, subject access, rectification, objection – but the introduction of a highly complex right to erasure (Article 17) has made 55% of organisations highlight it as the most pressing concern to GDPR-compliance.

The right to erasure is highly contentious. Even if we ignore the academic criticism that the European Court of Justice (ECJ) failed to "elaborate an accurate definition for the right to be forgotten" in Google Spain[22], and it offered some helpful indication as to the meaning of "inadequate, irrelevant, or excessive in the time that had elapsed"– namely, personal information regarded the forced sale of properties arising from social security debts – there is still a lack of case law on the right to be forgotten from the European Court of Human Rights (ECHR) and the ECJ. Moreover, as the GDPR has been in effect for only a year, there is still uncertainty over the exact burdens and obligations imposed on data controllers and processors. For example, what constitutes "reasonable

steps" to removing personal data which has been made public as per Article 17(2)? What should constitute a "necessary exercise" of the right to freedom of expression and information as per Article 17(3)(a), so to disapply controllers' obligation of erasing personal data?

Neville[23] and Szeghalmi[24] rightly both point out that these two rights necessarily conflict. Yet the balancing standard by the ECJ in *Google Spain* is nebulous: is there a right to erasure if the personal data relates to a public function or of public interest, as suggested in Springer?[25] If so, what does the "public interest" mean – does it include quasi-personal issues such as taxation matters?[26] Are we expecting too much of organisations who are unfamiliar with data compliance to look into even murkier areas of law, or even comparative legal material such as *Sidis v. FR Publishing Corp* from the US?[27] These are complex dimensions of law to which experienced judges do not have a comprehensive answer. Therefore, it is an unenviable task for organisations to familiarise, or even speculate, about their obligations – which will inevitably incur greater legal costs and impede them from achieving a competitive advantage in the first place. Again, this is hardly convincing for companies to buy into the narrative of "GDPR-compliance" being a "competitive advantage".

Conclusion

In conclusion, whilst GDPR-compliance should be seen as an opportunity by all organisations to secure a competitive advantage, it is viewed with scepticism due to the legal challenges the GDPR poses and realities of markets and industries. Therefore, there is some way to go before GDPR-compliance, and privacy law compliance as a whole is universally recognized as a ready-made competitive advantage.

AUTHOR

Alvin Cheung is a second year BA Jurisprudence student at University College, Oxford.

REFERENCES

1 General Data Protection Regulation (EU) 2016/679 of 25 May 2018 [2018] OJ L 127.
2 Organisation for Economic Cooperation and Development, Data-Driven Innovation for Growth and Well-Being: Interim Synthesis Report, October 2014, 11, ezproxy-prd.bodleian.ox.ac.uk:2160/sti/inno/data-driven-innovation-interim-synthesis.pdf
3 Duncan Brown, Ready or Not? GDPR Maturity Across Vertical Industries, International Data Corporation, April 2017, 3, https://us.blackberry.com/content/dam/blackberry-com/PDF/enterprise/wp-gdpr-maturity.pdf
4 GDPR, Article 25(1).
5 James Clark, "Legislative Comment – GDPR Series: anonymisation and pseudonymisation" (2017) 18(1) *Privacy & Data Protection*, 11.
6 Kelly Martin, Abhishek Borah, and Robert W Palmatier, "Research: A Strong Privacy Policy Can Save Company Millions" (*Harvard Business Review*, 15 February, 2018) hbr.org/2018/02/research-a-strong-privacy-policy-can-save-your-company-millions.
7 Kate Fazzini, "The great Equifax mystery: 17 months later, the stolen data has never been found, and experts are starting to suspect a spy scheme" (CNBC, 13 February 2019) https://www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html.
8 Paige Leskin, "The 21 scariest data breaches of 2018" (*Business Insider*, 30 December 2018) www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12?r=US&IR=T#8-google-525-million-14
9 Sead Fadilpašić, "Poor data practices can ruin a company, research claims" (ITProPortal, 8 February, 2018) www.itproportal.com/news/poor-data-practices-can-ruin-a-company-research-claims
10 "Fines and Penalties", (GDPR EU.ORG) www.gdpreu.org/compliance/fines-and-penalties/
11 Nader Henein, "GDPR: How to Make it a Competitive Advantage" (CSO from IDG, 16 November 2017) www.csoonline.com/article/3237646/gdpr-how-to-make-it-a-competitive-advantage.html
12 Maurice E. Stucke, Allen P. Grunes, *Big Data and Competition Policy*, (OUP 2016).
13 Federal Trade Commission, "FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network" (Press Release, 30 March 2011) www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz
14 Federal Trade Commission, "Google Will Pay $22.5 Million to Settle Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser" (Press Release, 9 August 2012) www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-
15 Casey Newton, "Google Reaches $7 Million Settlement with States over Street View Case" (CNET, 12 March 2013) http://www.cnet.com/news/google-reaches-7-million-settlement-with-states-over-street-view-case/
16 Federal Trade Commission, "FTC Approves Final Order in Case About Google Billing for Kids' In-App Charges Without Parental Consent" (Press Release, 5 December 2014) https://www.ftc.gov/news-events/press-releases/2014/12/ftc-approves-final-order-case-about-google-billing-kids-app
17 Stucke, Grunes, Big Data and Competition Policy.
18 Joseph Farrell, "Can Privacy Be Just Another Good?" (2012) 10 Journaal on Telecomm & High Tech Law 258-9.
19 Amy Gesenhues, "Facebook ad revenue keeps rising, 3 million advertisers using Stories Ads" (*MarketingLand*, 25 April 2019) marketingland.com/facebook-ad-revenue-keeps-rising-3-million-advertisers-using-stories-ads-259965
20 Calum Docherty, Fiona McLean and Danielle van der Merwe, "Legislative Comment – GDPR series: the new data subject rights" (2017) 17(8) *Privacy and Data Protection*, 9-11.
21 Data Protective Directive (Directive 95/46/EC) of 13 December 1995 (1995) L281
22 Case C-131/12, Google Spain SL v Agencia Española de Protección de Datos [2014] ECJ 317.
23 Andrew Neville "Is it a Human Right to be Forgotten? Conceptualising the World View" (2017) 15 Santa Clara J. Int'l L 157.
24 Veronika Szeghalmi, "Difficulties Regarding the Right to be Forgotten in the Case Law of the Strasbourg Court" (2018) 4(3) *Athens Journal of Law*, 267
25 *Fressoz and Roire v. France* (App no. 29183/95) on 21 January 1999.
26 *Axel Springer AG v. Germany* (App no. 39954/08) on 7 February 2012.
27 *Sidis v F-R Publishing Corporation* 311 U.S. 711 61 S. Ct. 393 85 L. Ed. 462 1940 U.S (US).

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 125+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 125+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Global Data Protection Officer, Dentsu Aegis Network**"

Subscription Fees

Single User Access

International Reports **£560 + VAT***
UK Reports **£450 + VAT***
UK & International Reports **£900 + VAT***
* VAT only applies to UK based subscribers

Multi User Access

Discounts for Multiple User licence (up to 10) and Enterprise licence (unlimited users).

Subscription Discounts

Introductory discount (first year): 30% off for DPAs, public sector, charities, academic institutions, use code SUB30; 20% off for other organisations, use code SUB20.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £25, Outside Europe = £35

Combined International and UK Editions
Rest of Europe = £50, Outside Europe = £70

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK