CSCI 2390 Privacy-Conscious Computer Systems: GDPR Case Study
2018-07-06, AggregateIQ (Canada), UK

Brandon Tan (tjiansin)
Brown University

Irvin Lim (ilim5)
Brown University

Abstract

This study examines the GDPR enforcement case of *AggregateIQ Data Services Ltd.* (AIQ), the first of its kind outside of the European Union (EU). The Information Commissioner's Office (ICO) of the UK found AIQ to be in violation of Articles 5 (1)(a)-(c) and Article 6 of the GDPR. AIQ then appealed the enforcement notice citing the ICO's lack of evidence, lack of clarity, inaccurate characterization of its businesses and the overlapping legal jurisdictions between the Office of Information and Privacy Commissioner (OIPC) of British Columbia and the ICO. The notice was revised and the case concludes with AIQ withdrawing its appeal and expressing its intention to voluntarily comply with the new notice. We then drew several observations about the proceedings of the case and provided suggestions on why things turned out the way they did.

1 Background

AggregateIQ Data Services Ltd. (AIQ) is a political consultancy and technology company based in Canada. Their customer base consists of mainly politicians and political organizations that are in active election campaigns. These political entities would contract AIQ, which provides services including "audience outreach, message testing, public opinion polling, online engagement and intervention, and audience analysis" [1].

Notably, AIQ has been linked to the Facebook-Cambridge Analytica scandal and is claimed to have been deeply involved in the United Kingdom's (UK) European Union (EU) Referendum vote in 2016 [2], which voted by a narrow margin in favor of the UK leaving the EU. AIQ's clients included Vote Leave, the official campaign for leading the "Leave" vote for the referendum, and has been shown to have had close ties to Cambridge Analytica [3]. AIQ also became the first international firm to have been served a formal enforcement notice for breaching the General Data Protection Regulation (GDPR) laid out by the EU in May 2018, which was issued by the Data Protection Agency (DPA) in the UK, the Information Commissioner's Office (ICO), dated on 6 July 2018 [4].

While little is known on AIQ's technical stack due to the controversial and hence secretive nature of the work they are doing, a security lapse on their code repository revealed some insights. From the repository, AIQ seems to be involved in the creating/hosting of campaign websites/apps of politicians and political organizations from Canada, USA and UK [5]. In addition, it was revealed that AIQ has developed or is in possession of a suite of tools that allows them to track, scrape, monitor and target advertisements at specific individuals and groups given some user data inputs, as well as their Facebook friends [6].

2 GDPR Violation

2.1 Details of the Case

The ICO issued its official enforcement notice on 31 May 2018, deeming AIQ, as both a data controller and processor of the personal data of UK individuals (the "data subjects"), to have breached several articles in the GDPR [4]. In particular, the notice outlines the subjects' email addresses and names as some of the personal data that was held on to by AIQ, which was confirmed to have still been in their possession as of 31 May 2018, 6 days after the GDPR took effect in the EU on 25 May 2018.

The ICO notice found that AIQ is in violation of Articles 5 (1)(a)-(c) and Article 6 of the GDPR [7]. Specifically, AIQ had failed to process personal data in a "lawful" manner (with respect to Article 6), in a way and for purposes that data subjects were not aware of or had agreed to when the data was originally collected.

In particular, AIQ was deemed to have run and paid for 2,823 different targeted advertisements on Facebook leading up to the referendum vote in June 2016, most of which were run on behalf of Vote Leave, amounting to around $2 million in total [2]. The main purpose of the advertisements were thought to push voters' inclinations and influence the result

of the 2016 Referendum with often provoking messages and specific issues [8]. The ads were directed to individual UK Facebook users by their email address as the primary targeting criteria, but the source of the dataset of email addresses used to target these ads toward remains unknown. AIQ was deemed to have still had access to this data on 31 May 2018 (the date of the notice), and ICO has since demanded AIQ to cease processing of the data through the enforcement notice.

ICO has also stated that the penalty could be up to 20 million Euros or 4% of AIQ's total annual worldwide turnover, whichever is higher.

2.2 AIQ's Appeal and ICO's Second Notice

In response to the enforcement notice, AIQ had since appealed against it. It claims that there has not been any evidence of "processing" of the UK personal data that it obtained from the various campaigns and has held on to after GDPR came into effect on 25 May 2018, apart for the purposes of "monitoring" [9]. To this effect, AIQ is claiming that it not only was not a data controller, but is also not a data processor since it had not "processed" the data, thus absolving it from complying with Article 5 and 6 of the GDPR. It further claims that there was a lack of precision on how it could comply with ICO's requirements, as well as how AIQ, being a Canadian firm, was not subject to UK's ICO but instead the Office of Information and Privacy Commissioner (OIPC) of British Columbia, which has conflicting requirements to *not* destroy the data [10].

However, ICO followed up with a subsequent enforcement notice on 24 October 2018, clarifying some of the above claims [11]. It instructed AIQ to "erase any personal data of individuals in the UK", and also cleared up the confusion of jurisdiction authorities by additionally stating to comply with notice within 30 days only after it is not subjected to OIPC investigations or if OIPC decides it is alright for AIQ to comply with the notice (whichever is sooner) [10].

Following the second notice, AIQ withdrew its appeal and co-founder Jeff Silvester commented that the company is happy to voluntarily comply with the new notice [13].

3 Discussion

3.1 Significance of the Case

Since this case is the first GDPR enforcement outside of the EU, it is likely to be significant in setting a precedent for future cases to be raised against non-EU organizations and individuals with the GDPR. As raised by AIQ in its appeal, it claims that non-EU firms would not be subject to EU's laws but instead only those in its own country and province, but yet ICO still manages to claim jurisdiction over the OIPC and reclaim its authority over AIQ. This raises questions about the scope of the GDPR itself, and how the legal boundaries might not be as clear as companies like AIQ might perceive it to be.

Furthermore, AIQ being an instrumental link to the result of the 2016 referendum and its controversial means to influence votes, as well as its ties to Cambridge Analytica (CA), and by extension CA's involvement in the 2016 US presidential election), it seems to be one of the largest and most significant cases to date where the GDPR has been enforced.

While the case concluded with AIQ complying, it nevertheless sets a precedent of what is to be expected from the ICO and for how the GDPR could be used as a powerful legal instrument by government authorities. This case would undoubtedly serve as a good reference for the future cases to come.

3.2 Thoughts on ICO's Demands

3.2.1 Ex Post Facto

While the misuse of personal data towards the purpose of micro-targeted ads had very obviously breached the GDPR had it been in place during 2016, but as mentioned by AIQ in its appeal, there had been no evidence whatsoever of AIQ doing anything with the data after that. While we are not lawyers, retrospectively penalizing the AIQ with a newly minted law based on its past actions seems to be "*ex post facto*", which is prohibited by Article 7 of the European Convention of Human Rights [12]. As such, much of the legal basis that ICO has for enforcing the GDPR seems to be the fact that AIQ holding onto the personal data is considered to be "unlawful processing".

3.2.2 Debatable "Processing"

While the exact degree of "processing" of the data, that was claimed by ICO to still have been done by AIQ after the GDPR had come into effect on 25 May 2018, is debatable, it also seems that the surprisingly short timeframe between the date of effect and the date of the enforcement notice (6 days) may suggest that the ICO intended to use the GDPR merely as a powerful means to take legal action against AIQ, considering the broad and fuzzy interpretation of the new law in practice at that time. This is also especially so considering that the ICO has been investigating AIQ and its involvement in the 2016 referendum since early 2017 [2].

3.2.3 Fine Enforcement Feasibility

Though the case concludes without AIQ being fined, it would be interesting to see how the ICO could have systematically enforced the fine on an international firm. At this point, the GDPR is more or less a paper tiger, which may cause a handful of companies to take some preemptive action to avoid such cases happening to them in the future. But given how AIQ's involvement and spotlight resulted only from a significant

whistleblowing case that involved both AIQ and Cambridge Analytica, international companies may very well just take the gamble and watch how things play out in the long run. More concrete enforcement techniques/frameworks need to be in place especially for companies based outside of the EU, and as demonstrated in this case, partnership with the local DPAs in the companies' respective jurisdictions would also help to streamline enforcement of the GDPR around the world.

3.2.4 A Tap on the Wrist

While not specifically referring to this AIQ case, the ICO's potential maximum fine of 20 million Euros or 4% global annual turnover generally seems to be a tad light. This is especially so when taking into account companies such as AIQ and Cambridge Analytica which actively engage in political engineering and may contribute to the destabilization of political systems throughout the world. The people they could potentially affect is not limited to the people that they have data of, but also the people of entire countries and regions.

While it seems that the ICO is doing everything it can to try to take proper legal action against AIQ for its involvement in influencing voters in the 2016 referendum, we feel that the proper legal instruments have to be used, instead of blindly enforcing the GDPR ex post facto. The larger takeaway from this case seems to be that regulations need to keep up with the times and introduce appropriately harsh penalties on companies that may engage in micro-targeting of voters via social media in the future.

References

[1] AggregateIQ Data Services Ltd., AggregateIQ (2019). Retrieved from https://aggregateiq.com/.

[2] Information Commissioner's Office, Investigation into the use of data analytics in political campaigns (2018). Retrieved from https://ico.org.uk/media/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf.

[3] Cadwalldr, C. (2017). Follow the data: does a legal document link Brexit campaigns to US billionaire?. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2017/may/14/robert-mercer-cambridge-analytica-leave-eu-referendum-brexit-campaigns.

[4] Information Commissioner's Office, *Enforcement Notice*. Received by AggregateIQ Data Services Ltd. ("AIQ") on 6 July 2018. Retrieved from https://ico.org.uk/media/2259362/r-letter-ico-to-aiq-060718.pdf.

[5] UpGuard, Inc., *The Aggregate IQ Files, Part One: How a Political Engineering Firm Exposed Their Code Base* (2018). Retrieved from https://www.upguard.com/breaches/aggregate-iq-part-one.

[6] UpGuard, Inc., *The AggregateIQ Files, Part Three: A Monarch, A Peasant, and a Saga* (2018). Retrieved from https://www.upguard.com/breaches/aggregate-iq-part-three-monarch.

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union L119* (May 2016), pages 1–88. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC.

[8] BBC (2019). Vote Leave's targeted Brexit ads released by Facebook. Retrieved from https://www.bbc.com/news/uk-politics-44966969.

[9] Townsend, K. (2018). First GDPR Enforcement is Followed by First GDPR Appeal. Retrieved from https://www.securityweek.com/first-gdpr-enforcement-followed-first-gdpr-appeal.

[10] Townsend, K. (2018). UK Regulator Issues Second GDPR Enforcement Notice on Canadian Firm. Retrieved from https://www.securityweek.com/uk-regulator-issues-second-gdpr-enforcement-notice-canadian-firm.

[11] Information Commissioner's Office, *Enforcement Notice*. Received by AggregateIQ Data Services Ltd. ("AIQ") on 24 October 2018. Retrieved from https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260123/aggregate-iq-en-20181024.pdf.

[12] European Court of Human Rights, *European Convention on Human Rights*. Retrieved from https://www.echr.coe.int/Documents/Convention_ENG.pdf.

[13] GlobalDataReview. (2018). ICO narrows first-ever GDPR enforcement notice. Retrieved from https://globaldatareview.com/article/1176139/ico-narrows-first-ever-gdpr-enforcement-notice.