The Consumer Voice in Europe

EUROPEAN PARLIAMENT HEARING ON THE USE OF FACEBOOK USERS' DATA BY CAMBRIDGE ANALYTICA AND ITS IMPACT ON DATA PROTECTION - 25.06.2018

Testimonial by The European Consumer Organisation (BEUC)
Represented by Ursula Pachl, Deputy Director General

Contact: directorsoffice@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • consumers@beuc.eu • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2018-067 - 09/07/2018

What are the consequences for consumers' trust in digital platforms and cybersecurity

- **Firstly**, it is clear that everything that this scandal is uncovering has and should have major consequences when it comes to **consumer trust**. Because this scandal is affecting consumer trust, not only regarding Facebook, but regarding the whole architecture of the digital economy. This is the perspective that we need to take.

- The way things work now, is that the exploitation of data is the primary source of revenue on the Internet. There is no doubt that it is not only on Facebook where the misuse of data might be happening, but across on-line platforms and the internet. The general feeling is that the transparency we need isn't there on platforms and that our data protection and privacy rights are not respected.

- **Secondly**, I would like to underline that this is **not only a matter of trust**. It is much more than that. It is our fundamental rights that are not being respected. **The practices in the FB/CA scandal are not only a breach of trust, they are illegal.**

Facebook case

- According to Facebook's official communication, 2.7M Europeans have been affected. 2.7M Europeans whose personal data was taken without their knowledge or informed consent, then sold on and used for a complete different purpose than the one that was initially established. It is puzzling that Facebook today repeatedly states that Dr Kogan collected data of European users, but did not share them with Cambridge Analytica.

- We are talking about the case of Cambridge Analytica here but Facebook has now already suspended over 200 apps for potential data misuse. Even if all these apps apparently came from a handful of developers, we are only looking at the tip of the iceberg.

- We can safely assume that if you are on Facebook, your data has been misused by someone at some point. All Facebook users are affected by the platform's lax approach to privacy protection and even people beyond, who have never had a Facebook account, given the pervasiveness of Facebook's tracking and profiling all across the web.

- For a long time, Facebook has been carelessly giving its users' data to third parties. And when it came to its knowledge that some people might be misusing that data, Facebook failed to take all the necessary measures to correct the situation.

- It has taken a major PR scandal and a lot of public pressure for the company to fully acknowledge the problem. And the company's response until now is far from satisfactory: an 'apology' tour and some 'cosmetic' changes on the platform are not good enough.

- It looks like Facebook has to a great extent "disguised" some of the changes it has introduced as a direct reaction to the scandal, in an attempt to regain trust (from its users, from the public, from politicians, etc.), BUT many of them were purely GDPR compliance-related changes.

- On that opportunity, let me say that we nevertheless have serious doubts as to where Facebook is actually complying with the GDPR despite these changes.

What do we need to fix this problem?

- What we need (and to comply with GDPR) are not only cosmetic changes. We need substantial modifications that would affect the core business model of Facebook and the structure of its platform.

- And by extension, the same can be said **for the core business model and monetisation structure of the internet**. As long as commercial surveillance and surveillance-based advertising remain the bread and butter of the digital economy, it will be very difficult to trust companies like Facebook with our data. These companies have an inherent conflict of interest at their core.

How do consumers feel about this?

- Our member Which? just recently published a very interesting study[1] about the future of consumer data. It shows that there is a widespread **sense of disempowerment amongst consumers**.

- People are unsure about the impact that the use of data by these platforms has on them and whether it is worth trying, or whether it is possible at all, to take any action about practices that concern them. They feel particularly disempowered because their own behaviour may inadvertently cause themselves harm. Studies show that in such circumstances, consumers give up.

- *So people have questions, but they still use Facebook.* The reason is not that they don't care: the seasons are resignation, disempowerment and lack of competition and alternatives. There is no mainstream substitute for Facebook on the market.

- Leaving aside the legal consequences, scandals such as the one we are discussing today are certainly not helping increase trust. However, they are sadly helpful from another perspective. They serve as **eye openers** for many people and help raise awareness about the underlying problems and the importance of privacy in the digital world.

[1] "Control, Alt or Delete? – The future of consumer data" - Which? Policy report, June 2018

Consumer damage

- Consumers start to wonder not only about whether companies respect their rights, but also about the **value of their data** and whether they are getting a fair deal from current market dynamics.

- It is also surprising, and to a certain degree disappointing, to see that in the whole debate around the Cambridge Analytica and larger Facebook scandal very little attention has been paid to the situation of consumers, despite it being their data that has been exploited and misused by Facebook. It's their privacy that was put at stake. They are the victims here.

- This is why, our Belgian, Italian, Spanish and Portuguese members – consumer organisations Test-Achats/Test-Aankoop, Altroconumo, OCU and DECO, have launched **today** or will launch in the coming days a collective redress action against Facebook, claiming economic compensation for Facebook users in their respective countries.

- In Belgium alone almost 20,000 people have already signed up. This is a ground-breaking action, which addresses a fundamental issue which remains largely unexplored until now: compensation for damages under data protection law. The action is also based on the breach of the EU unfair commercial practices directive.

- And it is not just about Cambridge Analytica. That's why these consumer groups (Test-Achats/Test-Aankoop, OCU, Altroconsumo, DECO) won't limit this class action to merely the consumers affected by the Cambridge Analytica scandal, but decided to represent all Facebook users. Although Facebook does admit that "personal user information has been improperly shared", it's very clear that they have no intention at all of compensating consumers for the misuse of their data. All consumers get so far is an apology.

Cybersecurity

- Coming back to trust. The equation is simple "No privacy = No Trust" // "No Trust = No success for the digital economy". The same can be said about **"(cyber)security**". This is another fundamental element in the equation. Closely related but different from privacy. My data needs to be safe from unwanted intrusions. If this is not the case I will not trust the service and I will not use it.

- Cybersecurity is key. However, let's not lose sight of what happened that brought us here. In the case of CA, Facebook's data was not 'stolen'. It is not like Facebook had forgotten to close the door of the office where it kept our data or that someone knocked down the door. The whole office was designed as an open space office, where, once allowed in by Facebook, you were free to walk around and take people's data and the data of their friends.

- What I said before about **consumer resignation** also applies to security breaches. Our members research[2] shows that consumers do not understand what happens to breached data. There is no assistance from companies or government to help them find out if their data has not only been stolen but also sold or otherwise publicly exposed. For example, credit card fraud is a major problem in this respect.

- Moreover, in a world of connected products that surround us (your smart home with the fridge, the TV, the camera, the doors, the heating, your childrens' toys, your car etc), privacy is at stake on and offline, *always*. Products spy on you, they record what you do, they transmit and sell your most private information. And: they can be easily hacked – much too easily as numerous report of our member organisations have shown.

- The IoT market is a failure with regard to security. But still we don't have any EU binding rules for product IT security in place or in preparation. And the European Commission has missed the opportunity to establish binding security by design and by default. The **Cybersecurity Act** that you are currently discussing and that will be voted in the lead ITRE committee will not solve problems for consumers. It is based on voluntary certification.

- It should be even clearer by now that we cannot simply rely on self-regulation and the 'apparent' good will of companies saying 'we value your privacy, trust us' and that they will protect our data, and our security. We need robust regulation.

- We have the GDPR, hopefully we will have an ePrivacy Regulation soon. The foundations are there. But we don't have rules on security.

Conclusions

1. Consumers need further support to **rebalance power** over the use of their data.

2. We firmly believe in the **GDPR** as a tool that will help change the game and help build up the trust that is currently missing. We need strong legal enforcement to force companies to change their practices and solidify the foundations upon which trust can really be built.

3. With a company that has a privacy track record as poor as **Facebook** and a business model which fully relies on the exploitation of people's data, we need more than apologies and some cosmetic controls that only give users an 'illusion' of control. **We call on the DPAs to undertake a thorough investigation against FB, also on current practices, so that the new consistency mechanism of the GDPR can be relied upon to establish a European enforcement response.**

4. **The European Commission should conduct a market study into the digital advertising market. Competition, data protection and consumer authorities should work together**.

5. **Compensation** of consumers for the misuse of their personal data should be self-understood. The GDPR doesn't provide for a collective redress instrument, but the European Commission has in April proposed the "New Consumer Deal", which includes a collective redress instrument that will also apply to data potation

[2] Cf footnote 1

infringements. We hope the European Parliament will support this proposal and progress on it quickly.

6. We need stronger measures to ensure **platform accountability for third-party access to data**. (Facebook apparently had no meaningful process, beyond terms and conditions, to monitor and enforce use of that data in line with terms and conditions.) Companies need to do more to ensure solid accountability structures for partner access to data and the further exploitation of these data.

7. Consumer organisations will contribute with complaints and legal actions to ensure that the digital lives that we all increasingly live can be lives in dignity, autonomy and trust. But we need collective redress tools for consumer organisations and we need civil society organisations that are strong in all European countries, which unfortunately is not the case at present.

END

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).