

Facebook and Data Privacy in the Age of Cambridge Analytica

APRIL 30, 2018 // AUTHOR: IGA KOZLOWSKA



In recent weeks, the world has been intently following the Cambridge Analytica revelations: millions of Facebook users' personal data was used, without their knowledge, to aide the political campaigns of conservative candidates in the 2016 election, including Donald Trump. While not exactly a data breach, from the public response to this incident, it is clear that the vast majority of Facebook users did not knowingly consent to have their personal information used in this way.

What is certain is that Facebook, the world's largest social network platform, serving over two billion customers globally, is facing public scrutiny like never before. With data breaches, ransomware attacks, and identity theft a regular occurrence in this digitally driven economy, this event is different. For the first time, we see the mishandling of social data for political purposes on a mass scale [1] It remains to be seen whether this will be a watershed moment for rethinking how

we use personal data in the modern age. It is also unclear whether this experience will change companies' and consumers' privacy practices forever. For now, however, Facebook users and investors, American and foreign governments, and numerous regulatory bodies are paying attention.

Cambridge Analytica and Facebook

In 2013, University of Cambridge psychology professor Dr. Aleksandr Kogan created an application called "thisisyourdigitallife." This app, offered on Facebook, provided users with a personality quiz. After a Facebook user downloads the app, it would start collecting that person's personal information such as profile information and Facebook activity (e.g., what content was "liked"). Around 300,000 people downloaded the app. But the data collection didn't stop there. Because the app also collected information about those users' friends, who had their privacy settings set to allow it, the app collected data from about 87 million people.[2]

Next, Dr. Kogan passed this data on to Strategic Communication Laboratories (SCL), which owns Cambridge Analytica (CA), a political consulting firm that uses data to determine voter personality traits and behavior.[3] It then uses this data to help conservative campaigns target online advertisements and messaging. It is precisely at this point of data transfer from Dr. Kogan to other third parties like CA that Dr. Kogan violated Facebook's terms of service, which prohibit the transfer or sale of data "to any ad network, data broker or other advertising or monetization-related service." [4]

When Facebook learned about this in 2015, it removed Kogan's app and demanded certifications from Kogan, and CA that they had deleted the data. Kogan and CA all certified to Facebook that they destroyed the data. However, copies of the data remained beyond Facebook's control. While Alexander Nix, the CEO of CA, has told lawmakers that the company does not have Facebook data, "a former employee said that he had recently seen hundreds of gigabytes on CA servers, and that the files were not encrypted" reports the New York Times.[5]

In 2015, Facebook did not make any public statements regarding the incident, nor did it inform those users whose data was shared with CA.[6] Neither did Facebook report the incident to Federal Trade Commission, the US agency that oversees privacy-related issues. As Mark Zuckerberg, Facebook CEO, said during his two-day Congressional hearing on April 9 and April 10, 2018, once they received CA's attestation that the data has been deleted and is no longer being used, Facebook considered the "case closed." [7]

With the breaking of the story on March 17, 2018 in *The Guardian*[8] and the *New York Times*[9], Facebook was made aware that the data in fact have not been purged to this day. The fallout from this incident has been unprecedented. Facebook is facing numerous lawsuits, US, UK, and EU governmental inquiries, a #DeleteFacebook boycott campaign, and a sharp drop in share price that's erased nearly \$50 billion of the company's market capitalization in a mere three days of the news breaking[10].

This is not the first time, however, that Facebook, has faced issues related to its data collection and processing.[11] And, it is not the first time that it has faced regulatory scrutiny. For example, in 2011, the FTC settled a 20-year consent decree with Facebook, having found that Facebook routinely deceived its users by sharing personal data with third parties that users thought was private.[12] It is only now that Facebook's irresponsible behavior is receiving widespread public scrutiny. Whereas warnings from privacy and security professionals to date have been large falling on deaf ears; why has this event capturing the attention of consumers, companies, and governments the world over?

We have seen international data breach cases at this scale before. Indeed, data breaches, identify theft, ransomware, and other cybersecurity attacks have become ubiquitous in a digital global economy that runs on data.[13] In the last five years, we have witnessed the 2013 Snowden revelations of mass global government surveillance and the 2014 North Korean attack on Sony, a US corporation.[14] The average consumer has been hit hard as well. The 2013 Target data breach resulted in 40 million compromised payment cards.[15] The 2016 Yahoo attack compromised 500 million accounts[16] and the 2017 Equifax hack compromised 143 million.[17] It doesn't help that, at the same time as the Cambridge Analytica incident, Facebook discovered a vulnerability in its search and account recovery features that may have allowed bad actors to harvest the public profile information of *most of its two billion users*. [18] It seems that the public feels that enough is enough.

Beyond the scale of the event, the Cambridge Analytica incident involves arguably the most serious misuse and mishandling of consumer data we've yet seen. The *purpose* for which the data was illegally harvested is new and it hits a nerve with an American society that is already politically divided and where political emotions run high. Funded by Robert Mercer, a prominent Republican donor, and Stephen Bannon, Trump's former political adviser, CA was using the data for explicit political purposes – to help conservative campaigns in the 2016 election, including Donald Trump's campaign.[19] Neither the 3000,000 Facebook users who downloaded the app nor their 87 million friends anticipated that their personal data could be used for these political purposes. It's one thing

if customer data is used to serve bothersome ads, or a hacker steals credit card information for economic gain, but it's another if the world's largest social network was taken advantage of to help elect the president of the United States. So what exactly is Facebook's accountability in all this?

From Data Breach to Breach of Trust

Was this incident a data breach? Facebook first responded on March 17, 2018 in a Facebook post by Paul Grewal, VP & Deputy General Counsel, who wrote that, "The claim that this is a data breach is completely false. Aleksandr Kogan requested and gained access to information from users who chose to sign up to his app, and everyone involved gave their consent. People knowingly provided their information, no systems were infiltrated, and no passwords or sensitive pieces of information were stolen or hacked."^[20] That same day, Alex Stamos, Facebook's Chief Security Officer, tweeted (and later deleted the tweet) that, "Kogan did not break into any systems, bypass any technical controls, our use a flaw in our software to gather more data than allowed. He did, however, misuse that data after he gathered it, but that does not retroactively make it a 'breach.'"^[21]

This is true. According to the International Organization for Standardization and the International Electrotechnical Commission – two bodies that govern global security best practices – the definition of data breach is as follows: "a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed."^[22] Because Facebook's systems were not penetrated and the data was mishandled by a third-party in explicit violation of Facebook's terms of service, the incident does not qualify as a data breach as understood by the global cybersecurity community. But what about everyone else?

Facebook quickly understood, however, that to millions of users whose data was mishandled, this incident *felt* like a data breach.^[23] Despite the fact that *technically* all 87 million Facebook users consented to Kogan's app collecting their personal data by not changing their privacy settings accordingly, the public outcry reveals that they do not feel that they authorized the app to access their data, let alone share it with a third party like CA. Facebook's defense that it does provide users with controls to determine what types of data they want to share with which apps and what can be shared with apps that their friends use felt empty to customers who are largely unaware of these controls because Facebook does not make it easy to access them. Moreover, Facebook's privacy settings are by default not set for privacy. This is, at least in part, because, as was made clear in the Congressional hearings this month, Facebook's business model relies on app developers' access to their users' data for targeted advertising, which makes up over 90% of Facebook's revenue. In other words, Facebook's business model conflicts with privacy-friendly policies.^[24]

Quickly recognizing this, Facebook pivoted, took some responsibility, and rather than argue the fine points of data breach definitions, apologized for what was *experienced* by customers as a breach of trust. Only five days after the story broke, Zuckerberg wrote in a Facebook post, “This was a breach of trust between Kogan, Cambridge Analytica and Facebook. But it was also a breach of trust between Facebook and the people who share their data with us and expect us to protect it. We need to fix that.”[25] That week Facebook took out full-page ads in nine major US and international newspapers with the message: “This was a breach of trust and I’m sorry we didn’t do more at the time. I promise to do better for you.”[26] Recognizing the complex digital ecosystem Zuckerberg said in his opening remarks at the Congressional hearing that, “We didn’t take a broad enough view of what our responsibility is. That was a huge mistake, and it was my mistake.”[27]

This “apology tour,” as Senator Blumenthal dubbed it, will be meaningless without concrete policy changes.[28] Facebook has already instituted some changes. For example, they have tightened some of the APIs that allow apps to harvest data like information about which events a user hosts or attends, the groups to which they belong, and page posts and comments. Apps that have not been used in more than three months will no longer be able to collect user data.[29] In addition, Facebook will now be authorizing those who want to place political or issues ads on Facebook’s platform by validating their identity and location.[30] These ads will be marked as ads and will show who has paid for them. In addition, in June, Facebook plans to launch a public and searchable political ads archive.[31] Finally, Facebook has started a partnership with scholars who will work out a new model for academics to gain access to social media data for research purposes. The plan is to “form a commission which, as a trusted third party, receives access to all relevant firm information and systems, and then recruits independent academics to do research in specific areas following standard peer review protocols organized and funded by nonprofit foundations.”[32] This should not only allow scholars greater access to social data but also safeguard against its misuse, as in the case of Dr. Kogan, by clearly distinguishing between data use for scholarly research and data use for advertising and other secondary purposes.

It remains to be seen just how extensive and impactful Facebook’s policy changes will be. Zuckerberg’s performance at the Congressional hearings was reported positively by the media and Facebook’s stock price regained much of the value it lost since the Cambridge Analytica story broke. However, this is in part because the Senators did not ask specific and pointed questions on what compliance policies Facebook will actually implement.[33] For example, the conversation around the balance between short privacy notices that are reader-friendly and longer and more comprehensive notices written in “legalese” resulted in Zuckerberg signaling that he knows that this debate among privacy professionals exists but did not lead to a commitment by Facebook to make their privacy policies more transparent.[34]

When Zuckerberg did mention specific policy changes, not all of them were new changes responding to this incident. For example, Zuckerberg announced Facebook's application of the European General Data Protection Regulation (GDPR) to all Facebook customers, not just Europeans, as a heroic move of self-regulation.[35] However, it should not have taken Facebook this long to announce this position. Limiting the GDPR to EU citizens only, is not only shortsighted as the GDPR becomes *de facto* global privacy standard, but also unfair to non-EU citizens who would enjoy less privacy protections. In other words, while the Congressional hearing and Facebook's initial policy changes are a good start, this should only be the beginning of Facebook's journey toward improved transparency and data protection.

Lessons Learned

What are the lessons learned from the Cambridge Analytica incident for consumers, for companies, and for governments?

Consumers must recognize that their data has value. Consumers should educate themselves on how companies, especially ones that offer free service like Facebook and Google, use their personal data to drive their businesses. Consumers should read privacy notices and take advantage of the in-product user controls that most tech companies offer. Consumers should take advantage of their rights to request that a company let them view, edit, and delete their personal data because after all, consumers own their data, not companies. When companies engage in fraudulent or deceitful data handling practices, consumers should file complaints with the FTC or other appropriate regulatory bodies. Finally, consumers should advocate for more transparency and controls from companies and demand that their elected officials do more to protect privacy.

Companies that electronically process personal data – which is now practically every company in the world – must learn to better balance privacy risks with privacy controls. The riskier the data use, the more user controls are required. The more sensitive the data, the more protections should be put in place. Controls can include explicit consent, reader-friendly and prominent privacy notices, and privacy-friendly default settings. Company leaders should do more than just follow the letter of the law by putting themselves in their customers' shoes. How do customers *expect* their data to be used when they hand it over? Is consent given? And is it truly freely given, specific, informed, and unambiguous? Moreover, as Facebook learned the hard way, there will always be bad actors. When sharing data with third parties, companies would do well to go the extra mile and ensure that those companies are meeting the company's privacy requirements by investing in independent audits. When receiving data from third parties, companies should confirm that that data was collected in compliant manner, not by taking their vendors' word for it, but again, by conducting period audits.

And finally, governments, in this digitally connected global marketplace, must reform outdated legislation so that it addresses the modern complexities of international data usage and transfers. The European Union, for example, is setting a global example, through the General Data Protection Regulation that comes into effect May 25, 2018. Seven years in the making, this is a comprehensive piece of legislation that (1) expands data subjects' rights (2) enforces 72-hour data breach notifications (3) expands accountability measures and (4) improves enforcement capabilities through levying fines of up to 4% of global revenue. Although applicable only to European residents and citizens, most multi-national tech companies like Facebook, Google, and Microsoft are implementing these standards for all of their customers. However, it is high-time, that the US Congress find the political will to pass similar privacy protections for US consumers so that everyone can take advantage of the opportunities that come with the 21st century digital economy.

Endnotes

[1] For an account of Facebook's role in undermining democracy see: Vaidhyathan, Siva. 2018. *Antisocial Media: How Facebook Disconnects Us And Undermines Democracy*. Oxford University Press. See also Heilbing, Dirk *et al.* 2017. "Will Democracy Survive Big Data and Artificial Intelligence?" *Scientific American*. <https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/> Accessed 4/22/2018.

[2] Kang, Cecilia and Sheera Frenkel. "Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users." *The New York Times*. April 4, 2018. <https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html> Accessed 4/26/18.

[3] Rosenberg, Matthew *et al.* "How Trump Consultants Exploited the Facebook Data of Millions." *The New York Times*. March 17, 2018. <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> Accessed 4/26/18.

[4] Granville, Kevin. "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens." *The New York Times*. March 19, 2018. <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html> Accessed 4/15/18.

[5] Rosenberg, 2018.

[6] Rosenberg, 2018.

[7] "Facebook CEO Mark Zuckerberg Hearing on Data Privacy and Protection." C-SPAN. April 10, 2018. <https://www.c-span.org/video/?443543-1/facebook-ceo-mark-zuckerberg-testifies-data-protection%20Accessed%204/15/18> Accessed 4/26/18.

[8] Cadwalladr, Carole and Emma Graham-Harrison. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach." *The Guardian*. March 17, 2018. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> Accessed 4/26/18.

[9] Rosenberg, 2018.

[10] Mola, Rani. "Facebook has lost nearly \$50 billion in market cap since the data scandal." Recode. March 20, 2018. <https://www.recode.net/2018/3/20/17144130/facebook-stock-wall-street-billion-market-cap> Accessed 4/26/18

[11] For one of the earliest analyses of Facebook's privacy policies see Jones, Harvey and Jose Hiram Soltren. 2005. *Facebook: Threats to Privacy*. <http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf> Accessed 4/22/18. See also Fuchs, Christian. 2014. "Facebook: A Surveillance Threat to Privacy?" in *Social Media: A Critical Introduction*. London: Sage.

[12] "FTC Approves Final Settlement With Facebook." Federal Trade Commission. August, 10, 2012. <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook> Accessed 4/15/18.

[13] For more on security and privacy see Schneier, Bruce. 2016. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York. W. W. Norton & Company.

[14] "The Interview: A guide to the cyber attack on Hollywood." BBC. December 29, 2014. <http://www.bbc.com/news/entertainment-arts-30512032> Accessed 4/27/18.

[15] "Target cyberattack by overseas hackers may have compromised up to 40 million cards." *The Washington Post*. December 20, 2013. https://www.washingtonpost.com/business/economy/target-cyberattack-by-overseas-hackers-may-have-compromised-up-to-40-million-cards/2013/12/20/2c2943cc-69b5-11e3-a0b9-249bbb34602c_story.html?noredirect=on&utm_term=.2d3d9c763c06 Accessed 4/27/18.

[16] Fiegerman, Seth. "Yahoo says 500 million accounts stolen." CNN. September 23, 2016. <http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/index.html> Accessed 4/27/18.

- [17] Siegel Bernard, Tara *et al.* "Equifax Says Cyberattack May Have Affected 143 Million Users in the U.S." *The New York Times*. September 7, 2017.
<https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html> Accessed 4/27/18.
- [18] Kang and Frenkel, 2018.
- [19] Rosenberg, 2018.
- [20] Grewal, Paul. "Suspending Cambridge Analytica and SCL Group from Facebook." March 16, 2018. Facebook Newsroom. <https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/> Accessed 4/15/18.
- [21] Wagner, Kurt. "How Did Facebook Let Cambridge Analytica Get 50M Users' Data?" Newsfactor. March 21, 2018. https://newsfactor.com/story.xhtml?story_id=113000078MBA Accessed 4/15/18.
- [22] ISO/IEC 27040: 2015. International Organization for Standardization.
<https://www.iso.org/obp/ui/#iso:std:iso-iec:27040:ed-1:v1:en> Accessed 4/12/18.
- [23] On the ethics of social media data collection see Richterich, Annika. 2018. *The Big Data Agenda: Data Ethics and Critical Data Studies (Critical Digital and Social Media Studies Series)*. University of Westminster Press.
- [24] "Facebook CEO Mark Zuckerberg Hearing on Data Privacy and Protection." C-SPAN. April 10, 2018. <https://www.c-span.org/video/?443543-1/facebook-ceo-mark-zuckerberg-testifies-data-protection%20Accessed%204/15/18> Accessed 4/26/18.
- [25] Zuckerberg, Mark. Facebook Post. March 21, 2018.
<https://www.facebook.com/zuck/posts/10104712037900071> Accessed 4/15/18.
- [26] "Facebook Apologizes for Cambridge Analytica Scandal in Newspaper Ads." March 25, 2018. *TIME*. time.com/5214935/facebook-cambridge-analytica-apology-ads/ Accessed 4/15/18.
- [27] "Facebook CEO Mark Zuckerberg Hearing on Data Privacy and Protection." C-SPAN. April 10, 2018. <https://www.c-span.org/video/?443543-1/facebook-ceo-mark-zuckerberg-testifies-data-protection> Accessed 4/15/18.
- [28] Dennis, Steven T. and Sarah Frier. "Zuckerberg Defends Facebook's Value While Senators Question Apology." Bloomberg. April 10, 2018. <https://www.bloomberg.com/news/articles/2018-04-10/facebook-s-zuckerberg-warned-by-senators-of-privacy-nightmare> Accessed 4/27/18.

[29] Schroepfer, Mike. "An Update on Our Plans to Restrict Data Access on Facebook." Facebook Newsroom. April 4, 2018. <https://newsroom.fb.com/news/2018/04/restricting-data-access/> Accessed 4/22/2018.

[30] For a broader discussion of social media and political advertising see Napoli, Philip M. and Caplan, Robyn. 2016. "When Media Companies Insist They're Not Media Companies and Why It Matters for Communications Policy" https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2750148 Accessed 4/22/18.

[31] Goldman, Rob and Alex Himel. "Making Ads and Pages More Transparent." Facebook Newsroom. April 6, 2018. <https://newsroom.fb.com/news/2018/04/transparent-ads-and-pages/> Accessed 4/22/2018.

[32] King, Gary and Nathaniel Persily. Working Paper. "A New Model for Industry-Academic Partnerships." April 9, 2018. <https://gking.harvard.edu/partnerships> Accessed 4/22/2018.

[33] Member of the House of Representatives took a more aggressive line of questioning with Mark Zuckerberg. For example, Representative Joe Kennedy III poked holes in Facebook's persistent claim that Facebook users "own" their data by pointing to the massive amount of metadata that Facebook generates (beyond what the user directly generates) and then sells to advertisers. See Madrigal, Alexis C. "The Most Important Exchange of the Zuckerberg Hearing." *The Atlantic*. April 11, 2018. <https://www.theatlantic.com/technology/archive/2018/04/the-most-important-exchange-of-the-zuckerberg-hearing/557795/> Accessed 4/27/18.

[34] For the evolution of Facebook's privacy policy see Shore, Jennifer and Jill Steinman. 2015. "Did You Really Agree to That? The Evolution of Facebook's Privacy Policy" *Technology Science*. <https://techscience.org/a/2015081102/> Accessed 4/22/18. For a broader conversation around privacy and human behavior see Acquisti, Alessandro. 2015. "Privacy and Human Behavior in the Age of Information" *Science*. Vol. 347. Pp. 509-514.

[35] For more on European privacy law see Voss, W. Gregory. 2017. "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting" *Business Lawyer*, Vol. 72. Pp. 221-233.

This publication was made possible in part by a grant from Carnegie Corporation of New York. The statements made and views expressed are solely the responsibility of the author.

About the Author

Iga Kozłowska

Dr. Iga Kozłowska is a sociologist and a privacy professional currently working in the technology industry. Iga's expertise in international technology issues is grounded in the unique perspective of a scholar and practitioner. Fascinated by the global digital economy and information governance, Iga is also interested in cybersecurity and is an Associate of the International Information System Security Certification Consortium, the world's leading cybersecurity and IT security professional organization. Iga completed her PhD in sociology at Northwestern University in 2017. Her dissertation research focused on the transnational diffusion of historical memories as it has impacted European integration since 2000. Iga received the US Fulbright Award (Poland 2015-2016) in recognition of the contributions of her research to the burgeoning field of transnationalism studies and to policymakers interested in fostering international cooperation and mutual understanding. Her prior research at the intersections of public policy and nationalism has been published in *Nations and Nationalism*.

TOPICS //

[Center for Global Studies](#)

[Cybersecurity](#)

[Disinformation](#)

[International Policy Institute](#)

[Privacy](#)

[Social media](#)

REGIONS //

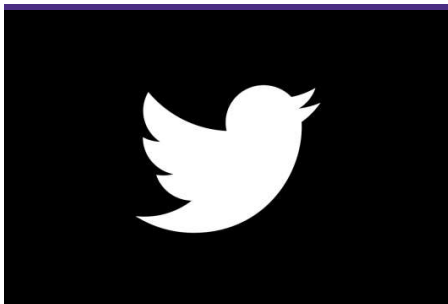
[Global](#)

[North America](#)

RESEARCH THEMES //

[Science and Technology](#)

RELATED ARTICLES



JSIS Cybersecurity Report: How Should the Tech Industry Address Terrorist Use of Its



Contextualizing the iPhone Encryption Debate



Countering Disinformation: Russia's Infowar in Ukraine

Products?

Latest News

[Scott Radnitz on how conspiracy theories in Russia work // .coda](#)

[Nadine Fabbi co-authors book chapter on the Inuit homeland and policy space in Canada](#)

[Scott Montgomery dives into why eliminating coal is so difficult in the Global South // Global Policy](#)

[Glennys Young quoted on legacy of UW's Red Square and the Cold War era // UW Daily](#)

[New handbook of gender in South Asia by Jackson School Director Leela Fernandes](#)

RELATED CENTERS
