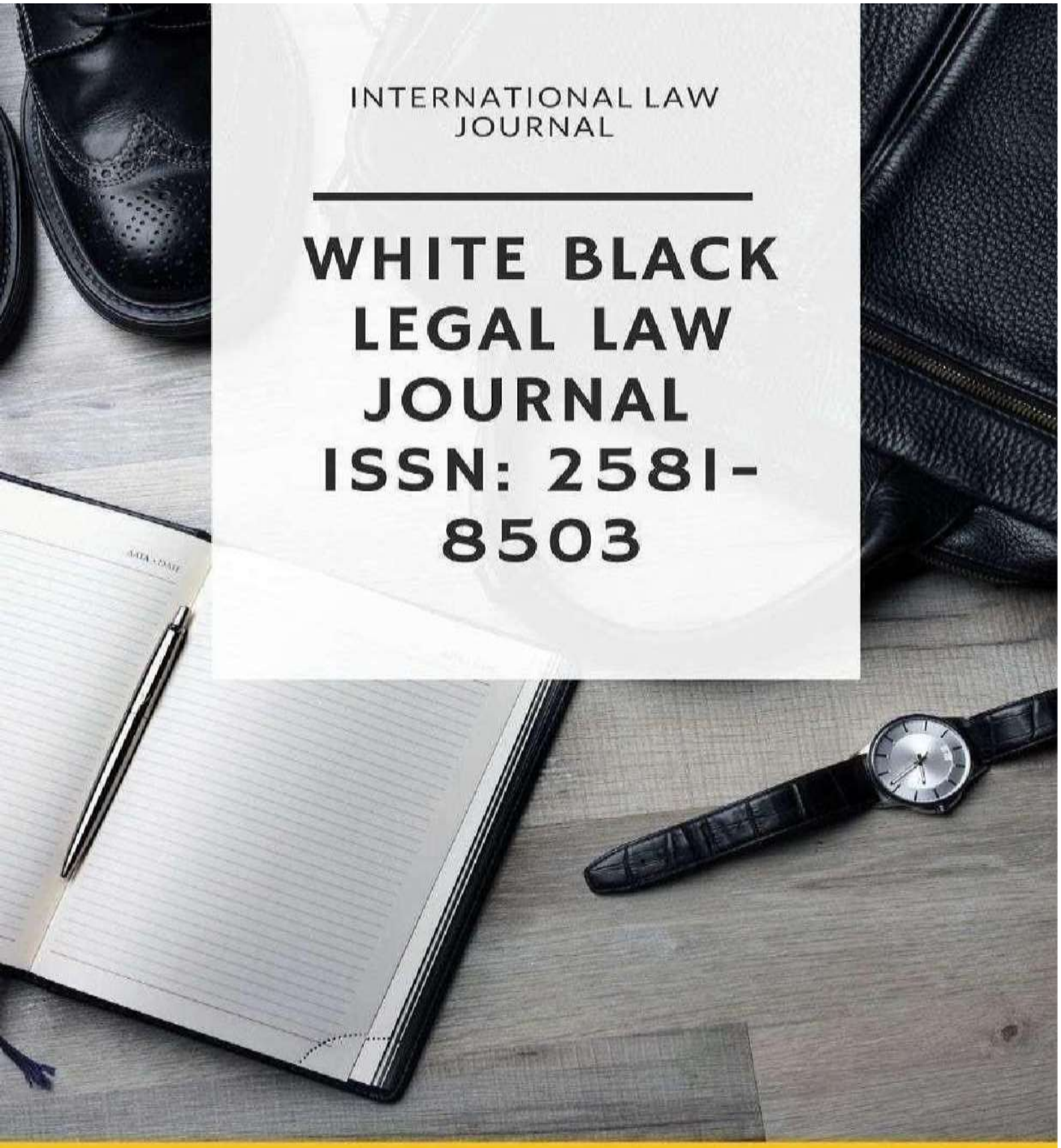

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

FROM CONSUMERS TO COMMODITIES: THE CAMBRIDGE ANALYTICA SCANDAL

AUTHORED BY - NISHITA MANIMARAN

INTRODUCTION:

Cybercrime can be defined as a broad term encompassing various illegal activities carried out using computers, networks, or other digital devices. It serves as an umbrella terminology for numerous offences committed by cybercriminals. With no clear physical boundaries in the endless abyss of the digital sea, cybercrime extends across the globe, affecting individuals, businesses, and technical infrastructure worldwide. By exploiting the vulnerable cracks in cybersecurity at all levels, cybercriminals continuously adapt their tactics, keeping the authorities on their toes. Cybercrime is popularly known to occur in various forms, including hacking, phishing, identity theft, ransomware, malware attacks, and many others. But does it always have to be these overtly criminal actions to constitute a cybercrime? No. In my personal opinion, cyberspace is a wonderful invention of mankind that has proven to be useful for various activities ranging from educational to socialising, especially in the case of social media apps. In today's time, people of the world receive both entertainment and news from the same social media sources. It truly has become a multidimensional platform. But all that glitters is not gold.

CAMBRIDGE ANALYTICA SCANDAL:

As demonstrated by the infamous Cambridge Analytica scandal, where personal data belonging to millions of Facebook users was collected by a British consulting firm for political advertising without the informed consent of said users for that purpose.[1] One might ask? Here, what is a cybercrime, as there were no attacks or hacking involved? However, misuse of personal data is one of the biggest cybercrime problems that is being faced by us in the 21st century, as nothing on the internet as claimed, is protected or safe; but rather just an illusion of privacy.

To enlighten you more on this subject, before we delve into the timeline of the scandal and the deep impact it has on the framework of cyber law. Our persona online contains a lot of personal

[1] Chan, Rosalie, *"The Cambridge Analytica whistleblower explains how the firm used Facebook data to sway elections"*, BUSINESS INSIDEcybercrimeHere, R (Jan. 27, 2026, 7:00 PM), https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10.

details such as name, address, credit card details, and contact information. When this personal data is used improperly for illegal purposes, such as unauthorized access, collection, or use of someone's private information without consent, with the intent to commit a crime such as fraud, identity theft, or other malicious activities or in this case, a political ploy.

As of today, writing this essay, I realise the Cambridge Analytica scandal catapulted its way into the public eye almost 8 years ago. In wake of the scandal, the notions of political persuasion and data mining, which were mere conversation topics, became strikingly real for every Facebook user. Its aftermath sparked an angry outcry; making it instead a conversation being had at every home, news outlet, media channels or just anywhere people could express their opinions. It also led to a series of re-evaluations of data privacy ethics and highlighted the increasing influence of social media on electoral politics, and how that did not seem like a good sign for the democratic structure. The legacy of Cambridge Analytica continues to shape the landscape of digital democracy to this day.

TIMELINE OF EVENTS:

The inception of the scandal:

The story dates as far back as 2010, when Facebook launched the Open Graph API for developers. This API is said to enable one application to access the data or features of another. [2]With this new tool at their disposal, developers could now explore social connections between individuals and discover relationships based on shared interests and likes. This was a crucial moment in Facebook's trajectory, as for the first time the app allowed external developers to reach out to Facebook users and request their permission to access a large chunk of their personal data and, crucially, to access their Facebook friends' personal data too.[3]

What seems like just an innocent graph for understanding the target audience on the outside was much too convoluted on the inside. If the user accepted the request, these third-party apps would now have access to a user's name, gender, location, birthday, education, political preferences, relationship status, religious views, online chat status, basically every personal

[2]Maarten Hoffman, *Has Sheryl Sandberg been thrown off the glass cliff*, PLATINUM MEDIA GROUP (Jan. 27, 2026, 9:00 PM) https://www.platinummediagroup.co.uk/platinum-business-magazine/2019/03/has-sheryl-sandberg-been-throw-off-the-glass-cliff/.

[3] Meredith Sam, *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal*, CNN (Jan. 27, 2026, 9:15 PM),https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.

information that forms part of your digital footprint. In fact, with additional permissions, external sites could also gain access to a person's private messages. Imagine your most private innermost thoughts being accessible to a stranger; well, this was just the digital version of it. Less than five weeks after Facebook launched Open Graph API version 1.0 for developers, seeing the public outcry, Zuckerberg wrote an op-ed for the Washington Post, in which he vowed to resolve users' concerns about how their personal information was being accessed by whomever or for whatsoever [4]

To make you further understand how Open Graph was used, let's take a look at a relatively harmless app like Farmville. They would use the API so people could see which of their friends were also playing their game and how users might interact while in the app. Now let's take a look at a political example of President Obama's campaign,[5] in which they built an app that would connect known Obama supporters to potential supporters. The basic idea was that these people had something in common, such as being friends on Facebook or that they both liked a particular sports team, which would help forge new communities. In both these cases, the use of API was absolutely fine as it isn't used nefariously, therefore doesn't fall under the cybercrime purview of mismanagement of data.

But this technology, combined with a few other events such as in the year 2013, A Cambridge Professor named Aleksandr Kogan and his company Global Science Research made an innocent personality detector quiz app called "thisisyourdigitallife". [6]This app merely prompted users to answer questions for a psychological profile. Almost 300,000 users were thought to have been paid to take the psychological test. He used Facebook's API software to determine what are the factors that influence their behaviours and also gathered data from their Facebook friends, which reportedly resulted in Kogan having access to the data of millions of Facebook profiles.[7]

[4]Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, THE NEW YORK TIMES(Jan. 27, 2026, 9:30 PM), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html .

[5] Meghan Mccain, *Comparing Facebook data use by Obama, Cambridge Analytica* POLITIFACT, (Jan. 27, 2026, 10:30 PM), https://www.politifact.com/factchecks/2018/mar/22/meghan-mccain/comparing-facebook-data-use-obama-cambridge-analyt/ from the original on August 18, 2019.

[6] Louis Ashworth, *Who is Dr Aleksandr Kogan, the Cambridge academic accused of misusing Facebook data,* VARSITY (Jan. 27, 2026, 11:07 PM),https://www.varsity.co.uk/news/15192.

[7] Meredith Sam , *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal* ,CNN (Jan. 27, 2026, 11:43 PM),https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.

In 2011, Facebook acquired an agreement with the American Federal Trade Commission over consent for sharing user data. And in 2014, Facebook had adapted its rules to limit a developer's access to user data. This change, which was rightfully made to ensure a third party was not able to access a user's friends' data without gaining permission first, failed to be pre-emptive in nature as these rule changes were not retroactively imposed, and Kogan did not delete the data he had previously acquired.[8] And instead, is thought to have allegedly sold the said data to Cambridge Analytica, a company that is known to provide data-driven services to political campaigns. Cambridge Analytica claimed to be able to use Facebook data for its clients to better target political messages to people that could be influenced, also known as "microtargeting." E.g. If a User is concerned about immigration policy, then he or she will be targeted with the ads explaining how a particular party is working in that area. Or, a rich class will be targeted with ads on how well they are working on economic policies. The ads are well customised to fit users' psychographics, aimed to yield maximum results. [9] This is both a cyber and an electoral crime. Following which Cambridge Analytica proceeded to make use of the data for various political campaigns and analytically assisted the 2016 presidential campaigns of both Ted Cruz and Donald Trump.[10] Cambridge Analytica was also widely accused of interfering with the Brexit Referendum,[11] Although the official investigation recognised that the company was not involved "beyond some initial enquiries" and that "no significant breaches" took place regarding the Brexit standpoint but not the same can be said for political accusations.

Breaking the story:

In March of 2018, The New York Times, in collaboration with The Observer of London and The Guardian and with the help of a whistleblower, acquired a collection of internal documents from Cambridge Analytica. These documents revealed that the firm had former Trump adviser Stephen K. Bannon serving as a board member, and speculations that he had misused data obtained from Facebook to construct voter profiles. [12]This revelation led to an investigation

[8] Josh Constine, *Facebook Is Shutting Down Its API For Giving Your Friends' Data To Apps*,TECH CRUNCH (Jan. 27, 2026, 11:55 PM),https://techcrunch.com/2015/04/28/facebook-api-shut-down/.

[9] Harshil Kanakia, Giridhar Shenoy and Jimit Shah, *Cambridge Analytica – A Case Study*, 12, INDJST,3-4 (2019).

[10] Nicholas Confessore, *"Cambridge Analytica and Facebook: The Scandal and the Fallout So Far"*,THE NEW YORK TIMES (Jan. 30, 2026, 6:00 PM), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[11] Izabella Kaminska, *"Cambridge Analytica probe finds no evidence it misused data to influence Brexit"*, THE FINANCIAL TIMES (Jan. 30, 2026, 6:20 PM), https://www.ft.com/content/aa235c45-76fb-46fd-83da-0bdf0946de2d.

[12] Matthew Rosenberg, *How Trump Consultants Exploited the Facebook Data of Millions,* NEW YORK TIMES

into Cambridge Analytica and plunged Facebook into its most significant crisis to date. But the story unfolded in a much more systematic way, one of the finest accomplishments of investigative journalism. Facebook attempted to discredit the same by announcing the suspension of Cambridge Analytica and its affiliate, the SCL Group, from accessing all data on its platform. The company also objected to the incident being called an “internal leak” but rather characterised it as a "data breach," emphasising that they were not to be held responsible. Following this, the founder of Facebook, Mark Zuckerberg went on to address the public many times, assuring them, but it was too late to sugarcoat the issue. With the judiciary already involved, the truth shall prevail!

Around March-April, the fiasco geared up a notch, with the first known account of a report by The Times. The report detailed that the contractors of Cambridge Analytica were extremely eager to sell psychological profiles of American voters to political campaigns. The same was acquired through the private Facebook data of tens of millions of users and exposed the largest known leak in Facebook history. The fact to be noted here is that Cambridge Analytica had been cautioned by its own lawyer, Laurence Levy, regarding its employment of European and Canadian citizens on the campaign and that an action such as this would breach American election law. [13]

Nor the public or the lawmakers were willing to sit silent.[14] There was a huge surge of people deleting their Facebook accounts, and the hashtag #DeleteFacebook and #WheresZuck began trending on Twitter. [15]This expose also prompted an immediate response in Washington, where lawmakers called for Facebook’s chief executive, Mark Zuckerberg, to testify before Congress. The US senator, Richard Blumenthal, tweeted, “Wanton theft and chilling privacy invasion require immediate Congressional hearings - and action”. Democrats demanded an investigation into Cambridge Analytica’s role in providing analytics to the Trump campaign. And on the other side of this equation, British lawmakers began conducting an investigation into

(Jan. 30, 2026, 6:44 PM),https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[13]Rob Peterson, *How well does Facebook know you*, BARN RAISERS Jan. 30, 2026, 7:30 PM), https://barnraisersllc.com/2018/04/09/facebook-knows-gathers-information-likes/.

[14]Mathhew Rosenberg, *Facebook’s Role in Data Misuse Sets Off Storms on Two Continents,* NEW YORK TIMES(Jan. 30, 2026, 7:40 PM),https://www.nytimes.com/2018/03/18/us/cambridge-analytica-facebook-privacy-data.html.

[15] Kevin Roose, *Missing From Facebook’s Crisis: Mark Zuckerberg,* NEW YORK TIMES (Jan. 30, 2026, 7:45 PM),https://www.nytimes.com/2018/03/21/technology/mark-zuckerberg-facebook.html.

Cambridge Analytica's involvement in disinformation, and the Brexit referendum echoed these concerns. The Federal Trade Commission began its investigation into whether Facebook had violated an early agreement to safeguard user data.[16]

The investigations revealed links between the aforementioned scandal, Mr Trump, Brexit and Silicon Valley. Three completely different issues affected by one company, i.e. Cambridge Analytica. Now let's break these links down one by one, firstly regarding the link to Mr. Trump we have evidence to show ties between Cambridge Analytica and John Bolton, the staunch conservative who was appointed as national security adviser by President Trump. [17] It was said that they had supplied Bolton with a "super PAC" with early iterations of its Facebook-derived voter profiles, marking the fact that the election was skewed, which proved true for the first time since the expose. [18]Secondly regarding the Brexit accusations, The Times and The Observer reported that the 2016 Brexit campaign had indeed enlisted a Cambridge Analytica contractor to circumvent election spending limits. The story went on to implicate two senior advisers to Prime Minister Theresa May. Further, a former Cambridge Analytica employee, Christopher Wylie, confessed that the company played a pivotal role in swaying the referendum outcome in favour of Britain's decision of withdrawal from the European Union.[19] Lastly, the Silicon Valley link presents itself as an employee at Palantir Technologies, which is an intelligence contractor founded by Trump supporter and tech investor Peter Thiel. The said employee exposed the company to have assisted Cambridge Analytica in harvesting Facebook data.

In the entire fiasco, the investigative journalism taken up by all the platforms is the true hero who deserves credit for uncovering everything, as they provided the truth to millions of people. Reports from Wired, The New York Times, and The Observer initially reported that the leak

[16]Tapiwa Matthew Mutisi,*Facebook–Cambridge Analytica Data Scandal and The Fallout So Far*, INNOVATION VILLAGE (Jan. 30, 2026, 9:45 PM), https://innovation-village.com/facebook-cambridge-analytica-data-scandal-and-the-fallout-so-far/.

[17] Mathhew Rosenberg, *Bolton Was Early Beneficiary of Cambridge Analytica's Facebook Data,* NEW YORK TIMES (Jan. 30, 2026, 10:00 PM), https://www.nytimes.com/2018/03/23/us/politics/bolton-cambridge-analyticas-facebook-data.html.

[18] Harry Davies, *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*, THE GAURDIAN (Jan. 30, 2026, 10:40, who PM) https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data?TB_iframe=true.

[19] David Kirk Patrick, *Using Digital Firm, Brexit Campaigners Skirted Spending Laws, Ex-Employee Say, NEW YORK TIMES* (Jan. 31, 2026, 8:00 AM),https://www.nytimes.com/2018/03/24/world/europe/uk-brexit-vote-leave-shahmir-sanni.html .

had information on 50 million Facebook users. While Cambridge Analytica claimed to have collected data on only 30 million profiles, Facebook later confirmed that the number was significantly higher, potentially exceeding 87 million users[20][21]

The Legal Disposition:

In the Matter of Cambridge Analytica, LLC, FTC Matter No. 182-3107. The Federal Trade Commission, having reason to believe that Cambridge Analytica had violated the provisions of the Federal Trade Commission Act, in the public interest, held that this scandal resulted in violations of multiple laws. Including the Federal Trade Commission Act (FTC Act)[22]- by falsely representing its data protection practices and failing to safeguard users' personal information. Additionally, Facebook was also found to have violated the FTC's privacy orders from 2012, further exacerbating the scandal. Facebook would also face penalties for failing to protect users' personal information, which enabled Cambridge Analytica to harvest data without proper consent, violating the Data Protection Act 1998[23]. And as per the U.S. Securities and Exchange Commission (SEC) Act[24]Facebook was sued for misleading investors by downplaying the risks associated with the misuse of user data, constituting a violation. It also further in the docket (No. 9383**)** stated that:[25]

- Cambridge Analytica explicitly or implicitly represented that neither directly nor indirectly, their GSRApp did not collect any identifiable information from Facebook users who granted it authorisation. However, the GSRApp did, in fact, collect identifiable information from these users, including their Facebook User IDs. So, their statement was false and misleading.
- Cambridge Analytica pledged its adherence to the Privacy Shield principles, according to which it is required that if a company withdraws from the Privacy Shield framework,

[20] Issie Lapwosky *"Facebook Exposed 87 Million Users to Cambridge Analytica*". WIRED (Jan. 31, 2026, 9:00 AM), https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/.

[21] Matthew Rosenberg; Nicholas Confessore; Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, NEW YORK TIMES (Jan. 31, 2026, 8:00 AM),.https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[22] Federal Trade Commission Act, Pub. L. No. 63-203, 38 Stat. 717 (1914).

[23] Data Protection Act 1998, c. 29 (U.K.).

[24] Securities Exchange Act of 1934, Pub. L. No. 73-291, 48 Stat. 881 (1934).

[25] Complaint, In the Matter of Cambridge Analytica, LLC, FTC Docket No. 9383 (FTC July 24, 2019), available at -https://archive.org/stream/civ53332855/182_3107_cambridge_analytica_administrative_complaint_7-24-19_djvu.txt.

it must affirm to the Department of Commerce that it will continue to uphold these principles. Which, in this case, was not complied with[26]

Following this, the Federal Trade Commission notified the alleged respondents on March 24, 2020, at 10:00 a.m. to appear. In one of those appearances, Mark Zuckerberg made his first appearance before Congress, [27]testifying before both Senate and the House committees. His initial session in the Senate saw intense questioning regarding Facebook's mishandling of user data, during which he revealed that the company was investigating "tens of thousands of apps" to determine the extent of data harvesting that had been undergone. At the second hearing, he faced even greater scrutiny in the House, where lawmakers largely agreed that social media technology and its potential for misuse had far outpaced regulatory oversight.[28] The discussion ended with the decision that the State must intervene to bridge this gap. Even Zuckerberg appeared to accept the same and was open to some form of regulation or oversight from the State, though neither he nor lawmakers had a clear vision of how to govern this new class of tech companies effectively.

INDIAN OVERVIEW

The Facebook–Cambridge Analytica scandal that we have been dealing with, as we know, represents a significant breach of data privacy. The Indian news media had been giving this controversy prime-time coverage. Had it happened in India instead of the USA, it would have violated multiple Indian laws. Including the Information Technology Act, 2000 (ITA) and constitutional privacy protections. Under Section 43A of the ITA[29], where companies are responsible for preventing unauthorised access to sensitive personal data, and Facebook's failure to do so is violative of the said provision. In fact, for the last several years, RSS ideologue Govindacharya has been filing PILs before the Delhi high court seeking to issue directions to Facebook and Google to comply with the Indian IT Act[30]. The Union IT minister Ravi Shankar Prasad has commented on the same saying, Indian laws are stringent and they

[26] United States of America Before The Federal Trade Commission (Plaintiff) V. Cambridge Analytica, Llc,A Corporation. (Respondent)

[27] Kevin Roose and Cecilia Kang , *Mark Zuckerberg Testifies on Facebook Before Skeptical Lawmakers,* NEW YORK TIMES (Feb.1, 2026, 6:00 PM)https://www.nytimes.com/2018/04/10/us/politics/zuckerberg-facebook-senate-hearing.html.

[28] Cecilia Kang and Kevin Roose, *Zuckerberg Faces Hostile Congress as Calls for Regulation Mount* NEW YORK TIMES (Feb.1, 2026, 6:30 PM)https://www.nytimes.com/2018/04/11/business/zuckerberg-facebook-congress.html.

[29] Information Technology Act, 2000, § 43 A, No. 21, Acts of Parliament, 2000 (India)

[30] Prashant Reddy, *Cambridge Analytica and Facebook – Is Anybody Actually Liable Under Indian Law?*WIRE (Feb.1, 2026, 8:00 PM)https://thewire.in/law/cambridge-analytica-facebook-liability-indian-law .

can summon Mr Zuckerberg.[31] Furthermore he also added that, India's federal investigating agency will determine whether personal data from Indian voters and Facebook users was compromised by the political consultant company Cambridge Analytica. This requirement is ignored by virtually all internet companies. The scandal also highlights a lack of transparency, and Indian law clearly mandates the need for disclosure of data collection and sharing practices, which Facebook failed to uphold, particularly in relation to third-party applications like Cambridge Analytica. Furthermore, the Indian Supreme Court's recognition of privacy as a fundamental right under Article 21(right to life and liberty) underscores the seriousness of this issue, as mishandling personal data could infringe upon this constitutional protection. [32] I do personally believe the Indian government takes issues such as data breaches seriously, as it could compromise the integrity and the sovereignty of the country. In fact, we have seen 59 Chinese apps being banned for the same reason, including the infamous ban of TikTok in India. But there is also an issue of a lack of due process being followed when it comes to these bans; the government needs to issue proper explanations, not an umbrella term of sovereignty and security. But an incident such as the Facebook scandal would have been dealt with much better under the Indian legal provisions, as we take the protection of the rights of citizens very seriously. Recently, it was reported that Meta had settled the case for 725 million, money prevailing over accountability, something I hope would not be the case in our country.

CONCLUSION & SUGGESTIONS:

The Facebook–Cambridge Analytica scandal serves as a stark reminder of the vulnerabilities that are associated with digital privacy and data protection. In today's world, there is a pressing need for stringent regulations and accountability in the handling of personal information by tech companies. The unauthorised collection and misuse of personal data not only violates legal statutes but also erodes public trust in digital platforms that have become an integral part of everyone's daily life and a trusted pathway to modern communication, commerce, and governance. Companies like Facebook operate on a global scale, amassing vast amounts of user data, yet their policies on data collection, storage, and sharing often lack clarity. Their biggest help is the lack of universal legislation regarding the same.

[31] Amit Baradwaj, *If an Indian party acted like Cambridge Analytica, it will not be guilty under current laws,*, NEWS LAUNDRY (Feb.2, 2026, 6:00 PM) https://www.newslaundry.com/2018/03/24/facebook-data-breach-cambridge-analytica-privacy-law-sunil-abraham,

[32] INDIA CONST. art. 21

This case showcases the need for collective effort from the government and the tech companies alike. There needs to be stricter regulations guarding users' personal data on both ends. Governments must focus on enforcement of the same, and corporates should take social responsibility for such scandals, together they can achieve the necessary. Understanding this, India has come up with the Data Protection Act 2023, hoping to address all these concerns so an incident like this wouldn't prevail in the Indian jurisdiction.