cognitio

studentisches Forum für Recht und Gesellschaft

Cambridge Analytica: A Property-Based Solution

CHIEH-JAN (SIMON) SUN

Zitiervorschlag

SUN, Cambridge Analytica: A Property-Based Solution, in: cognitio 2020/1.

URL: cognitio-zeitschrift.ch/2020-1/Sun

DOI: 10.5281/zenodo.3764717

ISSN: 2624-8417

cognitio

studentisches Forum für Recht und Gesellschaft

Cambridge Analytica: A Property-Based Solution

CHIEH-JAN (SIMON) SUN*

The 2018 Cambridge Analytica scandal exposed the concern that current privacy regulation is not sufficient to regulate data. In response, this paper proposes a property-based solution, arguing that only by recognizing the property right toward data, a more comprehensive regulatory system can be established. Concerning the current development of the information society, property rights should be granted toward Data Analytical Products and databases. Thus, as a new data regulation covering the two new types of data property will be constructed, the data-driven economy can be regulated and consumer privacy can be protected.

現行之隱私法規因2018年的劍橋分析事件而產生其不足以規範數據之疑慮。對此，本文建議應由物權之角度，透過肯認數據物權化之方式建立一更為完備之規範機制。考慮當代資訊社會之發展，物權宜被創設於數據商品及數據庫之中，並應以此為中心建立完整之管制模式，以規範數據經濟之發展及保護消費者隱私。

* LL.M. Candidate at Duke University School of Law, chiehjan.sun@duke.edu. The author initially submitted this paper in the course «Data and Democracy» lectured by Prof. Margaret Hu in Fall 2019. I want to thank Professor Margaret Hu for her supervision in this research paper and Professor Deborah A. DeMott and Professor Stuart Minor Benjamin for giving me the opportunity to present the paper in the Academic Workshop. I would also like to thank Professor Jeff Ward, Professor Jerome Reichman, Professor Jolynn Dellinger, Professor Nicole Ligon, and Mr. Keith Porcaro for all the valuable advice on this research paper. Finally, I am incredibly grateful for the support from the *cognitio* team as well as the Duke community, including Amna Al-naemi, Enning (Emelynn) Chang, Eun-Woo (Helena) Lee, Fabienne Graf, Xiuqi George Zhu, Hai Du, Inès Ndonko Nnoko, Jasmine Verma, Karim M'ziani, Kent Chen, Marine Tabory, Micheline George Deeik, Nur Kumru, Robert Hinz, Sangita Gazi, Yuan-Yuan (Avery) Chen and Yueh-Hsuan Lee.

Table of Contents

I. Introduction

Data is regulated through privacy law in the United States (U.S.). However, in the *Cambridge Analytica* scandal, millions of peoples' personal information have been exposed to third parties. Moreover, the data has been exploited to influence the 2016 U.S. presidential election. This revealed that the conventional data regulatory structure is inadequate to regulate information. In response, this paper explores the proposal of granting property rights toward data to protect the information, with a primary focus on the General Data Protection Regulation (GDPR), the current development of the Information Society, and prominent property theories. The aim is to construct a more comprehensive data regulatory regime.

This paper is divided into five sections. The first section will show how the *Cambridge Analytica* scandal exposed that traditional privacy laws may not be sufficient to regulate data. The primary focus will be placed on the challenges traditional privacy regulations have encountered. The second section will address the major approaches of recognizing data as property and an analysis of these approaches. This paper discovers that recent legislation has already covered certain aspects of these approaches. The third section will introduce the current development of the information society, including the rise of the database industry, the current application of data analytics, and the new data broker industry. Additionally, as Facebook is the center of the *Cambridge Analytica* scandal, the paper will explore the business model of Facebook. The fourth section will explore the possibility of granting property rights toward database and data analytics products and will discuss why property rights should be allocated toward companies instead of individuals. Also, this paper will discuss how the regulatory regime surrounding the two data properties should be constructed. Finally, this paper concludes that only by recognizing the property rights toward data, the data-driven economy and individual privacy can be protected.

II. Background: What Happened in Cambridge Analytica and Relative Regulations

A. Cambridge Analytica

The *Cambridge Analytica* scandal[1] broke on March 17th , 2018.[2] It was revealed that Cambridge Analytica, a data analytics firm that worked with 2016 United States presidential candidate Donald Trump's election campaign, had extracted Facebook users' data from 87 million user accounts.[3] Eventually, Facebook settles with the Federal Trade Commission (FTC) with a record-breaking $ 5 billion penalty.[4]

Users were asked to take a personality survey through an app developed by Aleksandr Kogan, a psychology researcher at Cambridge University.[5] The information about the users was further gathered based on a loophole in Facebook.[6] One of the

1 ROMANO AJA, The Facebook data breach wasn't a hack, It was a wake-up call, in: Vox from March 20, 2018.
2 ROMANO (Fn. 1).
3 ROMANO (Fn. 1).
4 Federal Trade Commission, FTC Imposes $ 5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, Press Release from July 24, 2019, Washington 2019.
5 ROMANO (Fn. 1).
6 ROMANO (Fn. 1).

most popular technologies offered by Facebook is *Facebook Login*, which lets people simply log in to a website or app using their account instead of creating new credentials.[7] However, when people use *Facebook Login*, they grant the app's developer access to a range of information from their Facebook profile.[8] This includes information such as their name, location, email, and friends list.[9] Things became problematic when Kogan shared all of these data with *Cambridge Analytica*, which is considered a violation of Facebook's terms of service.[10] *Cambridge Analytica* started harvesting users' data from millions of Facebook users and used that data to build a massive targeted marketing database based on each user's interests.[11] Using a personality profiling methodology, the company began offering its profiling system to dozens of political campaigns.[12] The targeting algorithms developed by *Cambridge Analytica* eventually influenced and predicted the voting behavior of the 2016 U.S. presidential election.[13]

Further, an investigation was launched into Facebook's consumer data privacy policies by the Federal Trade Commission (FTC), and an order to institute new privacy standards on Facebook was implemented.[14] The FTC's new 20-year settlement order overhauls the way the company makes privacy decisions by boosting the transparency of decision making and holding Facebook accountable through overlapping channels of compliance.[15] Facebook settled with the FTC in 2019 with an unprecedented $ 5 billion fine, which has been approved by the court on April 24th 2020.[16]

As a matter of fact, the *Cambridge Analytica* incident can be divided into three sections:

- The first section would be the fact that the app designed by Kogan has been harvesting users' information from Facebook.
- The second section would be both the transaction between the developer of the app and *Cambridge Analytica* as well as the transaction between *Cambridge Analytica* and the political campaign.
- The third section would be the fact that *Cambridge Analytica* has built a database based on Facebook's users' database and has analyzed users' voting behavior, which influenced the 2016 presidential election.

As the first section is related to traditional privacy regulation, the second and third section exceeds privacy protection as data has become a commodity for the companies. This incident raised the concern of whether traditional data regulation is adequate to protect consumers' data. Therefore, the following section will introduce the major data regulation in the U.S., followed by the various challenges these regulations have encountered.

B. Regulating Data Through Privacy Law

The protection of data in the U.S. is regulated through privacy law. Before *Cambridge Analytica*, prominent privacy regulations relative to consumer data protection include *Tort Law* and *Privacy Policies*.[17]

7 ROMANO (Fn. 1).
8 ROMANO (Fn. 1).
9 ROMANO (Fn. 1).
10 WAGNER KURT, Here's how Facebook allowed Cambridge Analytica to get data for 50 million users, in: Vox from March 17, 2018.
11 ROMANO (Fn. 1).
12 ROMANO (Fn. 1).
13 ROMANO (Fn. 1).
14 Federal Trade Commission (Fn. 4).
15 Federal Trade Commission (Fn. 4).
16 Federal Trade Commission FTC Chairman's Statement Regarding the Court's Approval of the Facebook Settlement, Press Release from April 24, 2020, Washington 2020.
17 SOLOVE DANIEL J./SCHWARTZ PAUL M., Information Privacy Law, New York 2018, 6th edition, p. 788.

Tort Law has been used primarily to encounter various forms of personal information collection, use, or disclosure in the U.S.[18] The establishment of privacy torts was born in a debate about property law, which initiated by WARREN and BRANDEIS in their Harvard Law Review article *The Right of Privacy* in 1890.[19] Property law at that time functioned as the protector of privacy.[20] Since one could not trespass, one could not invade the sanctity of the right to be left alone.[21] However, as people who lived in different conditions of the property, protecting privacy through the protection of property would no longer reach this goal.[22] Therefore, privacy should be separated from the property, and a new right – *The Right to Privacy* – was further proposed.[23] The article received a strong reception and recognition from courts as early as 1903.[24] Additionally, in 1960, as there were over 300 privacy tort cases decided since the WARREN and BRANDEIS article, Dean WILLIAM PROSSER examined and elaborated them into four types of privacy torts.[25] Those privacy torts include Intrusion upon Seclusion, Public Disclosure of Private Facts, False Light, and Appropriation.[26] This has been collectively known as *invasion of privacy* and has been commonly used in legal pleadings in modern tort law.[27]

Another major regulation of consumer data in the U.S. is *Privacy Policies*.[28] *Privacy Policies* are statements made by companies about their practices regarding personal information.[29] One of the common provisions is an opt-out provision, which establishes a default rule that the company can use or disclose the personal information how they want to as long as the consumer does not indicate otherwise.[30]Additionally, the FTC has deemed a violation of privacy policies to be an unfair or deceptive practice under section 5 of the FTC Act since the 1990s.[31] As the FTC cannot issue fines for violations of Section 5, the FTC can issue fines when companies violate a consent decree previously entered into for violation of Section 5.[32] The result was to make the U.S. a quasi-self-regulation system, in which companies would define the substantial terms of how they will collect, use, and disclose personal information, and be held accountable by the FTC.[33]

Overall, Privacy regulations before *Cambridge Analytica* have already been facing challenges on various grounds. First, as a massive amount of personal information is stored in private entities, individuals claiming privacy tort against commercial entities have been increasingly challenging.[34] It is hard to define the harm of the collection and usage of personal information, as one might argue that the kind of information that companies collect about individuals is not sensitive or intimate.[35] Moreover, companies may argue that consumers have consented to the use of information, and there was no injury since most users sign up for terms of use when they use the product.[36] In the case of *Cambridge Analytica*, the fact that users gave up their Facebook data coupled with the disclaimer from Facebook's user terms of

18 SOLOVE/SCHWARTZ (Fn. 17).
19 LESSIG LAWRENCE, Privacy as Property, in: Social Research 2002/69(1), Privacy in Post-Communist Europe, p. 247 et seq., p. 264.
20 LESSIG (Fn. 17).
21 LESSIG (Fn. 17).
22 LESSIG (Fn. 17).
23 WARREN SAMUEL D. BRANDEIS LOUIS D., The Right to Privacy, in: Harv. L. Rev. 1890/4, p. 193 et seq., p. 198.
24 SOLOVE/SCHWARTZ (Fn. 17), p. 25.
25 PROSSER WILLIAM, Privacy, in: Cal. L. Rev. 1960/48(3), p. 383 et seq.
26 PROSSER (Fn. 25).
27 SOLOVE/SCHWARTZ (Fn. 17), p. 20.
28 SOLOVE/SCHWARTZ (Fn. 17), P. 788.
29 SOLOVE/SCHWARTZ (Fn. 17), p. 829.
30 SOLOVE/SCHWARTZ (Fn. 17), p. 829.
31 SOLOVE/SCHWARTZ (Fn. 17), p. 789.
32 SOLOVE/SCHWARTZ (Fn. 17), p. 846.
33 SOLOVE/SCHWARTZ (Fn. 17), p. 787.
34 SOLOVE/SCHWARTZ (Fn. 17), p. 823.
35 SOLOVE/SCHWARTZ (Fn. 17), p. 823.
36 SOLOVE/SCHWARTZ (Fn. 17), p. 825.

service will make the claim of Facebook violating the promises unlikely to succeed.[37]

Second, the FTC has been criticized not to articulate its standard unambiguously, and the effectiveness of enforcement has been questioned.[38] Legal requirements are generally shrouded in mystery and have raised uncertain risk of enforcement discretion.[39] FTC settled with Facebook in light of *Cambridge Analytica*, which Facebook would have to pay a record-setting $ 5 billion penalty. However, the $ 5 billion fine will not go to any of the deceived Facebook users, but to the U.S. Treasury.[40] As FTC fails to cite any analysis of Facebook's unjust enrichment, critiques believe that the fine may not be hefty enough for Facebook to change its business model.[41] Moreover, FTC is unlikely to investigate the act of shaping users' political views by harvesting users' personal information, and such action can still happen in the future.[42]

As the *Cambridge Analytica* scandal has shown that traditional privacy regulation may not be adequate to protect consumer data, there is another branch discussion on privacy protection, which might be worth looking into. Some commentators proposed to grant property rights toward personal information to protect privacy. This branch of arguments has developed for more than 40 years, which can be categorized into four different approaches. The following section will introduce the major arguments of granting property rights toward data and provide an analysis of these proposals.

III. Theories on Property-Based Protection of Privacy

A. Major Approaches on Recognizing Property Rights Toward Data

Judge RICHARD POSNER first discussed the idea of granting property rights to information in his 1977 article, *The Right of Privacy*.[43] Judge POSNER proposes that every people's privacy and prying can be deemed as their economic goods, and people are assumed to use these goods as inputs into the production of income or some other broad measure of utility or welfare.[44] Property rights can be assigned in cases where secrecy is the byproduct of socially productive activity, and the disclosure of secrecy would impair the incentives to engage in that activity.[45] Property rights should be assigned away where the disclosure of secrecy would reduce the social product by misleading the people with whom he deals.[46] The legal right of privacy based on economic efficiency should include the protection of trade and business secrets by which people in business exploit their superior knowledge or skills.[47] There should be no protection for facts about people and the limitation would be of eavesdropping, and other forms of intrusive surveillance of illegal activities.[48]

Also supporting assigning property rights to privacy, Professor LAWRENCE LESSIG proposed to link the privacy protection architecture with the incentives of the market.[49] The property law is a regime where those who would use the data pay those whose data are

37 WOODS ANDREW KEANE, The Cambridge Analytica-Facebook Debacle: A Legal Primer, in: Lawfare from March 20, 2018.

38 STEGMAIER GERARD M./BARTNICK WENDELL, Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements, in: Geo. Mason L. Rev. 2013/20, p. 673 et seq.

39 STEGMAIER/BARTNICK (Fn. 38).

40 GILBERT BEN, Facebook was just slapped with a record-setting $ 5 billion fine for mishandling user data, but those users won't see a penny, Here's where that money goes, in: Business Insider from July 24, 2019.

41 CHOPRA ROHIT, Dissenting Statement of Commissioner Rohit Chopra, In re Facebook, Inc., Commission File No. 1823109 from July 24, 2019, p. 1.

42 CHOPRA (Fn. 41), p. 1.

43 POSNER RICHARD, The Right of Privacy, in: Georgia L. Rev. 1977/12, p. 393 et seq., p. 394.

44 POSNER (Fn. 43), p. 394.

45 POSNER (Fn. 43), p. 403.

46 POSNER (Fn. 43), p. 403.

47 POSNER (Fn. 43), p. 404.

48 POSNER (Fn. 43), p. 403.

49 LESSIG LAWRENCE, The Architecture of Privacy, in: Vand. J. Ent. L. & Prac. 1999/1, p. 56 et seq., p. 63.

being used.[50] If the law gave individuals the right to control their data, the market could negotiate these rights.[51] The benefit of a market is that the holder of the property right would have the power to hold out.[52] However, the cost of negotiating the price to be paid will be created.[53] Therefore, the architecture of this regime should be a Platform for Privacy Preferences (P3P) regime.[54] This is a standard designed by the World Wide Web Consortium (W3C) for negotiating protocols on the web, which would bear the cost of the negotiation process to protect individuals' privacy.[55]

Professor VERA BERGELSON argues that to protect privacy, individuals must secure control over their personal information by becoming its real owners.[56] Professor BERGELSON favors the property regime to protect private information mainly because «the torts approach cannot support a consistent, workable mechanism for the enforcement of information privacy rights.»[57] Such property rights should be allocated to the individual who generated personal information based on various property theories.[58] To balance the interest of the individual, society, and collectors, the interest of the individual in his personal information should not be a fee but rather a life estate.[59] Also, the collector should be granted a nonexclusive and unalienable automatic license in the collected personal information.[60] The original collector would have to obtain affirmative consent from the individual if they wanted to transfer personal information to a third party.[61] Further, the limitation on individual rights in personal information should come in the form of non-exclusive licenses in favor of society at large.[62] This limitation would allow the government to collect and transfer certain personal information, allow private and public noncommercial exchange by citizens, and permit public media to publish any newsworthy personal information without individual consent.[63]

Professor PAUL SCHWARTZ also supports the propertization of personal information and proposes a model to safeguard information privacy, which contains five elements.[64] First, inalienability should be imposed to restrict transferability.[65] Free alienability is problematic because of the information asymmetries about data collection and the use-transferability restriction run with the asset, which follows the personal information downstream.[66] Second, a mandatory opt-in default should be placed on the better-informed party to disclose material information about how personal information will be used.[67] This will force the hidden details on information processing to be disclosed.[68] Third, consent to information trade should imply both an initial opportunity to refuse trade and a later chance to exit from an agreement to trade.[69] A right of existing prevents initial bad bargains from having long-term consequences and preserves mobility for people to make use of privacy-enhancing opportunities or re-enter data trades.[70] Fourth, the State should be responsible for determining damages when harm occurs to information privacy interests.[71] It is hard to show actual damages in the context of privacy, and an individual's personal information may not have a high

50 LESSIG (Fn. 49), p. 64.
51 LESSIG (Fn. 49), p. 63.
52 LESSIG (Fn. 49), p. 63.
53 LESSIG (Fn. 49), p. 64.
54 LESSIG (Fn. 49), p. 64.
55 LESSIG (Fn. 49), p. 64.
56 BERGELSON VERA, It's Personal But is it Mine?, Toward Property Rights in Personal Information, in: U.C. Davis L. Rev. 2003/37, p. 382 et seq., p. 383.
57 BERGELSON (Fn. 56), p. 414.
58 BERGELSON (Fn. 56), p. 420.
59 BERGELSON (Fn. 56), p. 439.
60 BERGELSON (Fn. 56), p. 440.
61 BERGELSON (Fn. 56), p. 440.
62 BERGELSON (Fn. 56), p. 440.
63 BERGELSON (Fn. 56), p. 440.
64 SCHWARTZ PAUL M., Property, Privacy, and Personal Data, in: Harv. L. Rev. 2004/117, p. 2055 et seq., p. 2058.
65 SCHWARTZ (Fn. 64), p. 2095.
66 SCHWARTZ (Fn. 64), p. 2097.
67 SCHWARTZ (Fn. 64), p. 2100.
68 SCHWARTZ (Fn. 64), p. 2100.
69 SCHWARTZ (Fn. 64), p. 2106.
70 SCHWARTZ (Fn. 64), p. 2106.
71 SCHWARTZ (Fn. 64), p. 2106.

enough market value to justify the cost of litigation.[72] Fifth, institutions are needed to provide a trading mechanism, to verify claims to propertized personal information, and to police compliance with agreed-upon terms and legislatively mandated safeguards.[73] It should be a decentralized model, and the government should create a Data Protection Commission.[74]

B. Analysis on the Major Approaches

The approaches mentioned above vary on the mechanism designed for the propertized personal information. Interestingly, certain aspects of the proposals align with recent legislation enacted over the past few years.

Judge RICHARD POSNER's approach clearly demonstrates the case where property rights of information can be assigned to private individuals. Information such as trade secrets can be protected under this approach. The Uniform Trade Secrets Act (UTSA) was published by the Uniform Law Commission (ULC) in 1979.[75] The Defend Trade Secrets Act (DTSA) was further enacted on May 11, 2016, which for the first time, created a federal cause of action for misappropriating trade secrets.[76] These legislations show that Judge POSNER's understanding of propertized information, which emphasizes the protection of trade and business secrets, has been codified.

The other proposals rely on a market-based solution. The basic logic is that as individuals retain control over information, they will surrender less private Information during Internet transactions. However, the challenge of this approach is the existence of *Information asymmetries* between information collectors and individuals whose personal information is being collected.[77] Many individuals do not know how or whether the information is being processed and shared, and consumer ignorance could lead to a market in which one set of parties does not even know that negotiating is taking place.[78] Moreover, information collectors have an incentive to engage in tactics to make it difficult for individuals to obtain understandable information about the collection and usage of the process.[79] Once the imbalance of information causes a sufficiently large number of buyers to cease purchasing, problems with asymmetric information can be systematic enough to skew an entire class of negotiations.[80]

In response, Professor LESSIG endorses the Platform for Privacy Preferences (P3P) regime to bear the cost of negotiation and make it possible for the machine to act as our agents to protect privacy. However, the P3P has been criticized that it fails to comply with baseline standards for privacy protection and is deemed complex and confusing for Internet users by the Electronic Privacy Information Center (EPIC).[81] The key problem is that there is a lack of enforcement of the P3P.[82] Neither websites nor Internet users are obligated to use P3P.[83] EPIC also claims that P3P protocol would become burdensome for the browser and not as beneficial or efficient as it was intended to be.[84] Recently, Microsoft Internet Explorer, as the few major browsers that support P3P, has announced to end support from Windows 10 onwards.[85] Facebook published a statement stating that «[t]he organization that established P3P, the World Wide Web Consortium, suspended its work

72 SCHWARTZ (Fn. 64), p. 2109.
73 SCHWARTZ (Fn. 64), p. 2110.
74 SCHWARTZ (Fn. 64), p. 2111.
75 National Conference of Commissioners, Uniform State Laws Uniform Trade Secrets Act with 1985 Amendments, 16, p. 4.
76 American Bar Association (ABA), Explaining the Defend Trade Secrets Act, in: Business Law Today from September 20, 2016.
77 SCHWARTZ (Fn. 64), p. 2079.
78 SCHWARTZ (Fn. 64), p. 2079.
79 SCHWARTZ (Fn. 64), p. 2079.
80 SCHWARTZ (Fn. 64), p. 2079.
81 Electronic Privacy Information Center, Pretty Poor Privacy: An Assessment of P3P and Internet Privacy, Washington 2000.
82 Electronic Privacy Information Center (Fn. 81).
83 Electronic Privacy Information Center (Fn. 81).
84 Electronic Privacy Information Center (Fn. 81).
85 Microsoft, P3P is no longer supported, Support Change from December 15, 2016, Redmond 2016.

on this standard several years ago because most modern web browsers do not fully support P3P. As a result, the P3P standard is now out of date and does not reflect technologies that are currently in use on the web, so most websites currently do not have P3P policies.»[86]

Professor BERGELSON's proposal of requiring affirmative users' consent and Professor SCHWARTZ's proposal of adding the consent element into the propertized personal information are both a response to the *Information Asymmetries* dilemma. Fortunately, the General Data Protection Regulation (GDPR) was enacted on May 25th , 2018, right after the *Cambridge Analytica* incident exposed and puts in place strong restrictions on the use of consent requirements as a basis for processing personal information.[87] The GDPR requires that consent be «freely given, specific, informed and unambiguous.»[88] Mechanisms for gathering consent must be understandable and transparent.[89] Consent can be withdrawn at any time.[90] Additionally, the GDPR provides a right of correction and imposes temporal limits on data use.[91] The regulation permits the individual to obtain from the controller without undue delay the rectification of inaccurate personal information concerning him or her.[92] The regulation also creates a right to *erasure*, also known as *the Right to be forgotten*, which sets out several grounds that will trigger the controller's obligation to erase personal information.[93] Followed by the legislation of GDPR, the California Consumer Privacy Act (CCPA) has taken effect on January 1st, 2020.[94] This is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States.[95] Similar to the GDPR, the CCPA stresses the importance of more control over personal information to protect privacy.[96]

However, as the GDPR is designed to limit the power of Big Tech companies such as Facebook and Google, the policies implemented could make it difficult for smaller companies to thrive as big tech companies will have the resource to comply with all the requirements.[97] Rather than actually threatening big tech companies, the effect would minimize the threat of competition and make big tech companies' market positions more dominant.[98]
Similarly, as the CCPA tries to exclude small businesses from its requirements, the definition of *business* is still likely to reach many small businesses such as low-margin retail businesses and tiny ad-supported websites or blogs.[99] It is, therefore, critical to think of data regulation out of the scope of privacy law.

In order to develop a more comprehensive data regulatory regime, the following questions should be answered: First, what are the defining aspects of the era that we live in? It is essential to understand the economic activities that are related to data. This includes the underlying analytical method that has been used for analyzing data as well as the development of the data broker industry. Moreover, as Facebook is the center of the scandal, it would be crucial to understand Facebook's business model. Second, under this understanding of the information society, how should we characterize the usage of data? The discussion will focus on exploring various property theories supporting the creation of property and seeking the appro-

86 Facebook, Facebook's Platform for Privacy Preferences (P3P), Menlo Park from Feb 20, 2012 .
87 SOLOVE/SCHWARTZ (Fn. 17), p. 1169.
88 SOLOVE/SCHWARTZ (Fn. 17), p. 1170.
89 SOLOVE/SCHWARTZ (Fn. 17), p. 1170.
90 SOLOVE/SCHWARTZ (Fn. 17), p. 1170.
91 SOLOVE/SCHWARTZ (Fn. 17), p. 1169.
92 SOLOVE/SCHWARTZ (Fn. 17), p. 1169.
93 SOLOVE/SCHWARTZ (Fn. 17), p. 1169.
94 DataGuidance & Future of Privacy Forum, Comparing privacy laws: GDPR v. CCPA, London/Washington DC 2018, p. 5.
95 DataGuidance & Future of Privacy Forum (Fn. 94), p. 5.
96 DataGuidance & Future of Privacy Forum (Fn. 94), p. 5.
97 YUEH JEDIDIAH, GDPR Will Make Big Tech Even Bigger, in: Forbes from June 26, 2018.
98 YUEH (Fn. 97).
99 DETERMANN LOTHAR, An open letter to the California legislature on updating the CCPA, in: iapp from March 5, 2019.

priate legal regime to regulate data beyond privacy law. As mentioned above, the *Cambridge Analytica* incident can be divided into three sections. The goal of these questions would be to find the appropriate regulatory structure to cover all three sections. In particular, traditional privacy regulation does not fully cover the second and third sections of *Cambridge Analytica*, which concerns the transaction of the analytical product as well as the company's aggregative use of data that will ultimately influence the society.

IV. The Information Society: An Exploration of the Development of the Database Industry and the Facebook Business Model

A. The Rise of the Information Society

The rise of the *Information Society* comes with the demands of the growing public bureaucracies and private sectors' collection of information.[100] The federal government's endeavors at collecting data arose in its responsibility for conducting the census. On the other hand, the private sector's incentive was increasing competition in marketing.[101]

Census is an official count or survey of a population, typically recording various details of individuals.[102] By the 1970s, the U.S. began selling its census data on magnetic tapes to private sectors.[103] This can be understood as the rise of the data broker industry. To protect privacy, the Census Bureau sold the information on computer tapes in clusters of 1'500 households, supplying only addresses to protect privacy.[104] Within five years or purchasing the census data, these companies had constructed demographically segmented databases of over half of the households in the nation.[105] Today, federal agencies and departments maintain almost 2000 databases, including records about immigration, bankruptcy, Social Security, and military personnel.[106]

The rise of the database industry was also driven by the private sector's increasing advertising technique.[107] Marketers discovered targeted marketing as a new form of marketing, directed to discrete individuals or groups.[108] To increase the response rate, an effective way to collect, store, and analyze information ought to be done. The advent of databases provides an efficient way to store and search for data.[109] The databases enabled marketers to sort by various types of information and to rank or select various groups of individuals.[110] Companies such as credit card companies with databases started to realize that their databases are becoming one of their most valuable assets.[111]

As a massive amount of data is stored in the companies, a new form of a technique called *Data Analytics* started to develop, and companies were able to make data-driven decisions. *Data Analytics* refers to the set of quantitative and qualitative approaches to deriving valuable insights from data.[112] Various tools in *Data Analytics* can be deployed, and valuable insights of data can be successfully derived.[113] Currently, there are four primary types of data analytics, and each type has a different goal:[114] *Descriptive Analytics* summarize large datasets to describe outcomes and helps answer questions about what happened.[115] *Diagnostic Analytics* supplement more basic descriptive analytics.[116]

100 SOLOVE DANIEL J., Privacy and Power: Computer Databases and Metaphors for Information Privacy, in: Stan. L. Rev. 2001/53, p. 1400 et seq., p. 1462.
101 SOLOVE (Fn. 100), p. 1400.
102 SOLOVE (Fn. 100), p. 1400.
103 SOLOVE (Fn. 100), p. 1406.
104 SOLOVE (Fn. 100), p. 1406.
105 SOLOVE (Fn. 100), p. 1406.
106 SOLOVE (Fn. 100), p. 1403.
107 SOLOVE (Fn. 100), p. 1404.
108 SOLOVE (Fn. 100), p. 1405.
109 SOLOVE (Fn. 100), p. 1405.
110 SOLOVE (Fn. 100), p. 1405.
111 SOLOVE (Fn. 100), p. 1407.
112 Intellipaat, What is Data Analyitcs, in: IntelliPaat Blog from December 22, 2017.
113 Intellipaat (Fn. 112).
114 Master's in Data Science, What is Data Analytics?.
115 Master's in Data Science (Fn. 114).
116 Master's in Data Science (Fn. 114).

Predictive Analytics uses historical data to identify trends and helps answer questions about what will happen in the future.[117] *Prescriptive Analytics* uses insights from *Predictive Analytics* and helps answer questions about what should be done, which allows businesses to make data-driven decisions.[118]

Along with the growth of the database industry, another booming business is the formation of the data brokers companies. The FTC defines data brokers as «companies that collect information, including personal information about consumers, from a wide variety of sources to resell such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud.»[119] Much of the information data brokers collect is demographic, such as consumers' names, addresses, telephone numbers, email address, education level, gender, age, etc.[120] These data brokers obtain consumer data through avenues including government records, purchase or license from other data collectors, cooperative agreements with other companies, self-report by consumers, and social media.[121] None of the data brokers in the FTC report collected data directly from consumers.[122] Data brokers compile and analyze consumer data to create products that have a varying degree of specificity about individual consumers.[123]

117 Master's in Data Science (Fn. 114).
118 Master's in Data Science (Fn. 114).
119 Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers, Washington DC 2012, p. 68.
120 Committee on Commerce Science, and Transportation, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Washington DC 2013, p. 13.
121 Committee on Commerce Science (Fn. 120), p. 15.
122 Committee on Commerce Science (Fn. 120), p. 21.
123 MOHSIN MARYAM, 10 Facebook Stats Every Marketer Should Know in 2020, in: Oberlo from December 3, 2019.

B. The Facebook Business Model

Facebook is one of the most potent database builders in the world, with almost 2.5 billion monthly active users.[124] Facebook has made its products free to use by adopting a data-driven business model. The company has developed various methods to gather users' information and has been continuously improving its advertising tools.

Among all the tools managed by Facebook, the most controversial program was the system *Beacon*.[125] *Beacon* is a system whose primary purpose was to gather information about user activity on external websites to improve Facebook ad targeting.[126] When a Facebook user interacts with a *Beacon* partner website, the information would be sent to Facebook and would be reflected in the users' news feed.[127] However, user activities would appear in their Facebook feed even when the user was not connected to Facebook.[128] The system was withdrawn less than a year after launch as users found *Beacon* to be creepy – just imagine having «Just Searched for Shin Ramyun noodles on Amazon» showing up in your news feed.

In response, *Facebook Connect* was launched in late 2008, which is a product that allowed users to sign in to third-party sites with their Facebook credentials using the underlying technology of *Beacon*.[129] The value of *Connect* was enabling people to memorize a single, strong password for access to thousands of sites.[130] *Facebook Connect* led to a colossal improvement in ad targeting.[131] Facebook further introduced *Open Graph* in 2012, which leveraged its social graph.[132] This is a

124 CLEMENT J., Number of monthly active Facebook users worldwide as of 4th quarter 2019, in: Statista from April 30, 2020.
125 MCNAMEE ROGER, Zucked: Waking up to the Facebook Catastrophe, London 2019, p. 60.
126 MCNAMEE (Fn. 125), p. 60.
127 MCNAMEE (Fn. 125), p. 60.
128 MCNAMEE (Fn. 125), p. 60.
129 MCNAMEE (Fn. 125), p. 62.
130 MCNAMEE (Fn. 125), p. 62.
131 MCNAMEE (Fn. 125), p. 62.
132 MCNAMEE (Fn. 125), p. 70.

tool that captured everything it knew from both inside Facebook and around the web.[133] The introduction of *Open Graph* set the stage for better targeting, which improved rapidly as *off-site* data became available to advertisers.[134] At the same time, features of Facebook, such as photo tagging, news feed, also expanded the social graph.[135]

Additionally, new tools such as *Custom Audiences* and *Lookalike Audiences* were introduced. This enabled advertisers to connect Facebook users who share characteristics with the *Custom Audience* and to create a *Lookalike Audience*.[136] Also, data goes into Facebook's artificial intelligence and can be used by advertisers to exploit the emotions of users in ways that increase the likelihood to predict what the consumers would purchase.[137] Advertising on social media platforms has evolved into a form of manipulation.[138] To date, the company is still experimenting with algorithms, new data types, and small changes in design, measuring everything.[139] Facebook has made continuous improvements in its advertising tools, growing its audience, gathering an astonishing amount of information, which translated into explosive revenue growth.[140]

Based on the development of the Information Society and the Facebook business model, it can be concluded that the defining aspect of the data-driven economy is that data acquires value when it has been combined with other data through algorithms using analytical methods. The core would be the database of the company. Therefore, in order to characterize the usage of data, it will be critical to understanding prominent property theories and relevant regulatory regimes.

IV. Data Property: Creating and Regulating the Two New Types of Data Property

A. The Creation of Data Property

Property is created based on two streams of property theories, in which *economic value* and *personhood interest* play a dominant factor in consideration. The mainstream liberal market-based protection is the *Lockean Labor-Desert Theory* and the *Utilitarian Theory*:[141] The *Labor-Desert Theory* focuses on the acquisition of property through the investment of labor and the right of self-determination.[142] Therefore, people acquire a property right as they invest their labor in it. The *Utilitarian Theory* takes its primary purpose on maximizing personal benefit and confronts the problem of what constitutes benefit and how to measure it.[143] Under the *Utilitarian Theory*, property rights should be allocated to maximize personal satisfaction or benefit.[144] Under the *Labor-Desert Theory*, the self-actualization value of trade follows the investment of property. Under the *Utilitarian Theory*, people mutually-agreed exchanges are utility-enhancing of what people do is what they want.[145]

As both of these theories are dominant liberal market-based property theories, they converge on a vision of defining property through *economic value*.[146] It can be concluded that, once information has *economic value*, a property right toward information can be created. Ownership of the property would be allocated toward the parties that generate *economic value* from the property.

Coexisting with the dominant liberal market-based understanding of property are a variety of theories that deem property not solely

133 MCNAMEE (Fn. 125), p. 70.
134 MCNAMEE (Fn. 125), p. 70.
135 MCNAMEE (Fn. 125), p. 69.
136 MCNAMEE (Fn. 125), p. 77.
137 MCNAMEE (Fn. 125), p. 69.
138 MCNAMEE (Fn. 125), p. 69.
139 MCNAMEE (Fn. 125), p. 77.
140 MCNAMEE (Fn. 125), p. 77.

141 COHEN JULIE E., Examined Lives: Informational Privacy and the Subject As Object, in: Stan. L. Rev. 2000/52, p. 1373 et seq., p. 1379.
142 COHEN (Fn. 141), p. 1380.
143 COHEN (Fn. 141), p. 1381.
144 COHEN (Fn. 141), p. 1381.
145 COHEN (Fn. 141), p. 1381.
146 COHEN (Fn. 141), p. 1381.

by their *economic value* but rather by the ways they shape the social relations among persons.[147] In particular, MARGARET JANE RADIN's theory of property for personhood introduces two crucial arguments: The first argument is the idea that noneconomic or dignitary interests might preclude or restrict the transfer of property by its nominal owner.[148] The second argument is that if we think of these possessory interests as property, we acknowledge the possibility of a wholly new kind of concurrent estate.[149] Additionally, in terms of a party claiming a *personhood interest* on things possessed by another party, C. EDWIN BAKER and JOSEPH SINGER propose that we should ensure the individuals who are data subjects have greater power to control access to their transactional histories than third parties.[150] In short, personhood theory might support a dignity based claim to one's personal data.[151]

As the liberal market-based theory is the more dominant property theory, the traditional property-based solution of privacy seems to align with RADIN's theory of property. However, RADIN's theory may encounter difficulty applying to privacy regulation as the common way to protect the privacy of data subjects is «Pseudonymization.» The definition of pseudonymization under the GDPR and CCPA is very similar, which means the processing of personal data in such a manner that the personal data can no longer be attributed to an identified or identifiable person without the use of additional information, by putting in place technical and organizational measures which keep the additional information needed for identification separately.[152] As the biggest challenge of pseudonymization is re-identification, the GDPR and the CCPA requires that controllers and business cannot be obliged to re-identify datasets in order to be able to comply with their obligations.[153] The GDPR provides an exception to this rule concerning the rights of data subjects, to the extent that the additional information to re-identify the data is provided by the data subject himself or herself.[154] The CCPA states explicitly that the rule also applies in the case of the right of access.[155] As it is hard to re-identify the datasets, after the pseudonymization process, the *personhood interest* of the data shall be eliminated. Therefore, individuals may not be able to recognize property interest toward the anonymized information under MARGARET JANE RADIN's property theory.

At the same time, it is worth considering whether it is possible to claim ownership toward data based on the dominant liberal market theory, which focuses on the *economic value* that has been generated through the usage of data. This relates to the defining aspect of the information society mentioned above, which reveals that data becomes valuable when it has been combined with other data and has been analyzed through various data analytical methods. The result is either in the form of a product sold by data brokers or as an insight for companies to perfect their target marketing techniques. Since the real market exists among the aggregative use of data under the information society, property rights should be granted toward the analytical product that is being traded by data brokers and the database owned by companies. Specifically, the product being traded between data brokers can be termed as *Data Analytical Product*. At the same time, under a study done by the Financial Times, the average person's data often retails for less than a dollar.[156] Since so little *economic value* has been generated, it will be difficult to

147 COHEN (Fn. 141), p. 1382.
148 COHEN (Fn. 141), p. 1382.
149 COHEN (Fn. 141), p. 1382.
150 COHEN (Fn. 141), p. 1383.
151 COHEN (Fn. 141), p. 1382.
152 DataGuidance & Future of Privacy Forum (Fn. 94), p. 16.
153 DataGuidance & Future of Privacy Forum (Fn. 94), p. 16.
154 DataGuidance & Future of Privacy Forum (Fn. 94), p. 16.
155 DataGuidance & Future of Privacy Forum (Fn. 94), p. 16.
156 STEEL EMILY/LOCKE CALLUM/CADMAN EMILY/FREESE BEN, How much is your personal data worth?, in: Financial Times from June 12, 2013.

grant property rights toward individuals under the liberal market-based theory.

As mentioned above, trade secret a form of propertised information and is protected under the rule of law. Interestingly, the Uniform Trade Secrets Act (USTA) defines a trade secret as «information, including a formula, pattern, compilation, program, device, method, technique, or process that Derives independent *economic value*, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain *economic value* from its disclosure or use; and Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. » This definition also stresses the importance of *economic value*.

As the data analytical product and database should be deemed as property, the next question becomes, how should the new data regulatory regime be constructed based on this understanding of data property. The primary focus should be placed on the controversial second and third sections of the *Cambridge Analytica* incident, which relates to the transaction of users' information and the fact that *Cambridge Analytica* tempts to manipulate user behavior through the database they have built.

B. The Regulation of Data Property

1. Data Analytical Product

As the *Data Analytical Product* is being sold and traded between data brokers, it would be crucial to regulate data brokers based on the products that are being traded. Recently, Vermont's Act 171 of 2018 has been issued by the Vermont Office of the Attorney General on December 11th, 2018.[157] The new law requires Data Brokers to register with the Secretary of State annually and maintain specific minimum data security standards.[158] Information required to be registered includes a contact to whom acknowledgment that the information has been received, the name and primary physical, email, and internet addresses of the data broker.[159]

However, Vermont law does not require the types of analytical products to be provided. This is problematic as the product is the center of the data broker industry. Regulation on data brokers should not only be based on the characteristic of the entities that sell and trade data but should be based on the products that they sell. Fortunately, the FTC issued a report on Data Brokers in May 2014. The FTC has organized the legislative recommendations of data brokers based on the types of products.[160] Different types of products would have a different standard of transparency. Therefore, based on different products, a consumer would have different right to learn of the existence and activities of data brokers. Consumers would have reasonable access to information held by the entities. This characterization established by the FTC can serve as a useful guideline, which categorizes data products into three categories, including marketing products, risk mitigation products, and people search products:[161]

- Marketing products enable data brokers' clients to create tailored marketing messages to consumers.[162] The Commission has grouped these marketing products into (1) direct marketing, which encompasses postal mail, telemarketing, and email marketing; (2) online marketing, which includes marketing to consumers on the internet, on mobile

157 MELENDEZ STEVEN, A landmark Vermont law nudges over 120 data brokers out of the shadows, in: Fast Company from March 2, 2019.

158 The Vermont Office of the Attorney General, Guidance on Vermont's Act 171 of 2018 Data Broker Regulation, Montpelier 2018, p. 1.

159 The Vermont Office of the Attorney General (Fn. 158), p. 7.

160 Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability, Washington DC 2014, p. 46.

161 Federal Trade Commission (Fn. 160), p. 23.

162 Federal Trade Commission (Fn. 160), p. 23.

devices; and (3) marketing analytics, which enable a client to more accurately target consumers for an advertising campaign refine product and campaign messages, and gain insights and information about consumer attitudes and preferences.[163]

- Risk mitigation products can be grouped into two categories: (1) identity verification, which assists clients in confirming the identity of an individual; and (2) fraud detection, which helps their clients to identify or reduce fraud, assist entities in verifying the reliability or truthfulness of information a consumer submits to them, and assist companies that have had a data breach by analyzing patterns to determine whether there appears to be a misuse of the personal information breached.[164]
- People search products offer information about consumers obtained from government and other publicly available sources such as social media sites.[165] Individuals often use these products instead of organizations.[166] These products may allow a user to search with as little as one data element such as name, address, telephone number, email address, or SSN.[167]

In the *Cambridge Analytica* incident, the product the firm offered was the profiling information of the users. If the *Data Analytical Product* types were specified, and users were able to access their information, the problem would have been revealed in an early stage. In other words, with this regulation, the second section of the *Cambridge Analytica*, which deals with the transportation of the analytical product, can be covered.

163 Federal Trade Commission (Fn. 160), p. 31.
164 Federal Trade Commission (Fn. 160), p. 33.
165 Federal Trade Commission (Fn. 160), p. 34.
166 Federal Trade Commission (Fn. 160), p. 34.
167 Federal Trade Commission (Fn. 160), p. 35.

2. Database

Currently, the database of the company is protected under copyright law in the U.S. and the European Database Directive in the E.U. In particular, the European Database Directive grants a sui generis right toward the database besides copyright protection.[168] The essential feature of a sui generis right is about the substantial investment in the database and the protection against acts of extraction and re-utilization.[169] According to the Database Directive, any substantial change to the contents of the database that could be considered to be a new investment will cause the term of protection to run anew.[170] Given that databases are usually dynamic in a big data context, as data is continuously poured in, this could result in providing indefinite protection as all likelihood to substantial changes to the contents of the database.[171]

However, the jurisprudence of the Court of Justice of the European Union (CJEU) has clarified that an investment in the creation of the data as such does not suffice to merit protection under the sui generis right. Such reasoning would entail that the sui generis right does not apply to machine-generated databases, as it could be argued that the data included in such databases are created instead of obtained.[172] This would have a broader effect on the data economy, which relies on digitization processes such as the Internet of Things devices and artificial intelligence, as it becomes increasingly difficult to distinguish between the generation and the obtainment of data in the context of such processes.[173] It will become hard to satisfy the sui generis right protection requirements in a data economy context,

168 U.S. Copyright Office, Report on Legal Protection for Databases, 110, Washington DC August 1997, p. 45.
169 U.S. Copyright Office (Fn. 168), p. 46.
170 DEBUSSCHE JULIEN/CÉSAR JASMIEN, Big Data & Issues & Opportunities: Intellectual Property Rights, in: Bird & Bird from March 2019.
171 DEBUSSCHE/CÉSAR (Fn. 170).
172 DEBUSSCHE/CÉSAR (Fn. 170).
173 DEBUSSCHE/CÉSAR (Fn. 170).

given that the processes of obtaining, verifying, and presenting the data will happen more and more automatically.[174] It is, therefore, worth considering other possible approaches.

One considerable solution is to adapt to the *trust regime*. A trust is a fiduciary relationship in which the settlor gives the right to the trustee to hold title to a property (trust property) for the benefit of the beneficiary.[175] One basic principle of trust is that any right that has *economic value* can be a right held on trust. Therefore, the database is theoretically applicable to be treated as the trust property. This aligns with the argument of granting property rights toward the database builders. Also, this perfectly construes the fact that data is continuously poured into the database. Consequently, the company becomes the trustee, and the users become the beneficiaries. As the trustee owns the trust property, the trustee will owe fiduciary duties to the beneficiaries, and the beneficiaries will have the title to sue for damages.[176] This regime should be applied to companies which business model is built on the exploitation of users' data.

Additionally, there are several advantages of adapting a *trust regime* to regulate information: First, as mentioned above, a trust is a legal relationship in which a trustee runs the trust property for the benefit of the beneficiary. Under a *trust regime*, as the database will be viewed as trust property, all data beneficiaries will be able to claim the benefit of the trust property with considerable value.[177] This benefit can be termed as *Data Dividend*. However, there might be a difficulty for individuals to claim data dividend as there would be millions of data subjects having a claim on millions of different aggregate data trust.[178] In the future, a quantify system to decide the value of the benefit each people could acquire should be established, and a technological system for tracing and tracking the value of the data should be built.[179] Users should be able to seek guidance from an intelligent digital advisor to filter opportunities, and new regulatory infrastructure should be established.[180] In the meantime, it will be best to regard the benefits as a sort of aggregate pot, and the pot of benefits can be transformed into a new form of tax.[181] This could provide for statutory levels of compensation for privacy harms as tort liability is hard to establish in the modern era.[182] The tax could also serve as a fund for existing privacy regulatory entities such as the FTC.[183]

Second, under the trust regulatory system, as the data collector holds the information for the benefit of the data beneficiary, fiduciary duty will be imposed on the database owner.[184] As the database owner holds it for the benefit of the information beneficiary, they should act in the interest of the data subject.[185] Accordingly, based on Professor JACK BALKIN's *Information Fiduciary Theory*,[186] social media companies will hold three major duties, including the duty of care, the duty of confidentiality, and the duty of loyalty.[187] The first two duties require fiduciaries to secure customer data and not disclose it to anyone who does not agree to assume similar obligations.[188] The duty of loyalty requires the fiduciary not to seek to advantage themselves at their end-users' expense and must work to avoid creating a

174 DEBUSSCHE/CÉSAR (Fn. 170).

175 Shanda Consult, Cyprus International Trusts, Nicosia 2020.

176 EDWARDS LILIAN, The problem with Privacy: A modest Proposal, in: Int. Rev. Law Com. & Tech. 2004/18(3), p. 340 et seq., p. 327.

177 EDWARDS (Fn. 176), p. 328.

178 EDWARDS (Fn. 176), p. 328.

179 POSNER ERIC A./WEYL E. GLEN, Radical Markets: Uprooting Captialism and Democracy for a Just Society, Princeton 2018, p. 243.

180 POSNER/WEYL (Fn. 179), p. 245

181 EDWARDS (Fn. 176), p. 328.

182 EDWARDS (Fn. 176), p. 329.

183 EDWARDS (Fn. 176), p. 330.

184 EDWARDS (Fn. 176), p. 328.

185 EDWARDS (Fn. 176), p. 328.

186 BALKIN JACK M., Information Fiduciaries and the First Amendment, in: U.C. Davis L. Rev. 2016/49, p. 1183 et seq., p. 1221.

187 BALKIN JACK M., Fixing Social Media's Grand Bargain, Aegis Series Paper No. 1814, Stanford 2018, p. 13.

188 BALKIN (Fn. 187), p. 13.

conflict of interest.[189] Social Media Companies should not use end-user information psychologically manipulate them.

In the case of *Cambridge Analytica*, first, the tax could be posed on both *Cambridge Analytica* and Facebook. Consumers will be able to have new access to decent enforceable compensation rights when privacy harms occur.[190] This would be a good alternative for the $ 5 billion fine. Second, as an information fiduciary, both Facebook and *Cambridge Analytica* violated all three of its duties. In particular, Facebook did not take sufficient care to vet its business partners.[191] Facebook did not take adequate steps to audit the operations of the third parties and allowed third parties to manipulate its end users for profit.[192] Furthermore, when Facebook discovered what had happened, it did not take sufficient steps to protect its end-users from further breaches of confidentiality.[193] Therefore, under the trust approach, all three sections of the *Cambridge Analytica* incident are covered.

V. Conclusion

In conclusion, this paper has divided the *Cambridge Analytica* incident into three sections and has advocated for the creation of two new forms of data properties so that the three sections can be covered. Specifically, different from the traditional property-based approach of granting property rights toward data to users, this paper proposes to grant property rights toward Data Analytical Product and database to companies based on the *Lockean Labor-Desert Theory*.

It is critical to recognize property rights toward data so that it is easier to characterize the usage of that information. The property-based regulatory structure effectively regulates the Data Analytical Product as transparency of the property can be achieved. Moreover, as treating the database of the companies as their trust property perfectly construes the relationship between users and companies, companies will be imposed fiduciary duties to manage data, and users will be able to generate data dividend through companies' exploitation of data. Overall, if property right is not recognized, consumer privacy might be compromised, and the whole democratic system may be at risk.

189 BALKIN (Fn. 187), p. 13.
190 EDWARDS (Fn. 176), p. 330.
191 BALKIN (Fn. 187), p. 13.
192 BALKIN (Fn. 187), p. 13.
193 BALKIN (Fn. 187), p. 14.