Surveillance: The DNA of Platform Capital – The Case of Cambridge Analytica Put into Perspective

Ivan Manokha

Abstract

This paper places the case of Cambridge Analytica's theft of data from Facebook user profiles into a larger context of the growing importance of surveillance in modern-day capitalism. It argues that in the current phase of capitalism, data, particularly user data, is becoming a 'fictitious commodity' that is used by various commercial entities as the key 'raw material'. The operation of such entities, which is effectively based on continuous privacy invasions, is not brought into question and is actually normalized by those who oppose only covert data acquisition as in the case of Cambridge Analytica.

Introduction

On March 17, 2018, *The Observer of London*[1] and *The New York Times*[2] revealed that Cambridge Analytica, the London-based consulting group, had gathered private data from the Facebook profiles of more than 50 million users without their consent, the figure which later went up to 87 million.[3] The collection of data was carried out through a Facebook-based quiz app 'thisisyourdigitallife', created by Aleksandr Kogan, a University of Cambridge psychologist who gained access to information from 270,000 Facebook members after they had agreed to use the app to undergo a personality test, for which they were paid through Kogan's company, Global Science Research. But as Christopher Wylie, a Canadian data scientist and a former employee of Cambridge Analytica, stated,[4] the app could also collect all kinds of personal data from users (the content that they consulted or liked, and the messages that they posted). In addition, the app provided access to information on the profiles of the friends of each of those users who agreed to take the test, which explains the fact that 87 million users were affected. All this data was then shared by Kogan with Cambridge Analytica, which was working with Donald Trump's election team and which allegedly used this data to target US voters with personalised political messages exploiting what Cambridge Analytica "knew about them and targeting their inner demons".[5]

Following these revelations the internet has been engulfed in outrage to which government officials were quick to react. On March 19, Antonio Tajani, President of the European Parliament, stated in a twitter message that misuse of Facebook user data "is an unacceptable violation of our citizens' privacy rights" and promised an EU investigation.[6] On March 21, Brazil prosecutors opened an investigation into Cambridge Analytica,[7] and the following day Israel's Justice Ministry opened an inquiry into possible violations of Israelis' personal information by Facebook.[8] On March 27, Christopher Wylie appeared as a witness before the Digital, Culture, Media and Sport Committee of the British parliament and on April 10, 2018, Facebook director Mark Zuckerberg testified before the US Congress. Finally, on May 2, just forty-six days after the start of the scandal, Cambridge Analytica succumbed to the mounting public pressure and announced its closure, as well as the closure of its parent company, SCL Elections.[9]

Is the shutting down of Cambridge Analytica a triumph of different civil society activists in the fight against violations of individual privacy, or are we dealing with a 'pyrrhic victory'?[10] It seems plausible to argue that the latter is the case, as the actions of Cambridge Analytica is only one (and, comparatively, a rather minor one) of many instances of data collection and privacy violations routinely performed by different actors, especially by digital platforms; the only difference is that Cambridge Analytica attempted to use more covert measures to get access to individual data. The protesters and policy-makers have not questioned the conditions that render such cases possible and have not challenged the practice of routine and continuous data collection as a profit-making activity which has become normalized and which is now part of modern life.

It must be acknowledged that in academia there exist several studies which have tried to analyse and question modern practices of data collection and monetization using the notion of 'surveillance capitalism', first employed by Foster and McChesney,[11] and later developed by several other authors, particularly by Shoshana Zuboff,[12] who has contributed the most to the popularization of the term. However, the extent of this literature has so far been very limited - only a handful of journal articles - and by Zuboff's own admission the study of 'surveillance capitalism' and the "new social relations and politics" that it involves, has "not yet been well delineated or theorized".[13] More importantly, the available studies are marked by a range of notable shortcomings. To begin with, the developments

that they identify - increased amounts of data collected by private sector actors on customers, users, markets, and so on - in support of the claim that we now live in an era of 'surveillance capitalism' (and that it is different from previous phases of capitalism), are hardly novel and involve only quantitative changes. Thus, Zuboff, for example, argues that 'surveillance capitalism', which she defines as a "new form of information capitalism [which] aims to predict and modify human behavior as a means to produce revenue and market control" has arisen "during the last decade".[14]

This claim is problematic because consumer surveys, market research, loyalty cards and advertisement have existed for a very long time and their objective has always been to influence consumer choices. As Baran and Sweezy,[15] for example, observed in 1966, Fordist policies of higher wages right from the start came with attempts to manipulate workers into spending their money on (often wasteful) goods through advertisement, which played the central role in the rise of 'consumer culture' in the 1950s, as well marketing, which quickly became a complex system of consumer surveillance and targeting. The same criticism may be directed at Foster and McChesney who link the rise of 'surveillance capitalism' to the US "military-imperial dominance and capital accumulation" in the post-war period, which "naturally led" to the creation of internal enemies and their surveillance.[16] According to them, with the advent of financialization of the 1980s, the private sector, and particularly banks, intensified data collection on customers, which led to the further strengthening of 'surveillance capitalism'. In this respect, to the criticisms made with respect to Zuboff, here we may add that state bureaucracy and related practices of surveillance have been one of the central characteristics of Western modernity[17] and may hardly be said to have started in the post-war period in the US.

In addition, Zuboff asserts that the previous stages of capitalism were characterized by "the dynamism of a market democracy"[18] while the advent of 'surveillance capitalism' reconfigures "the structure of power, conformity, and resistance inherited from mass society and symbolized for over half a century as Big Brother. Power can no longer be summarized by that totalitarian symbol of centralized command and control. Even the panopticon of Bentham's design ... is prosaic compared to this new architecture".[19] It is important to remember that in capitalism the market has always been a realm of compulsion and unfreedom for the dominant majority of people who do not own any means of production, except their 'human capital', and who must sell their labour power for a wage to subsist.[20] In addition, surveillance has always been at the heart of the wage-labour relation and employers have continuously attempted to bring the time actually worked by laborers as close as possible to the time for which they are paid (one of the best known such attempts is 'time and motion' studies of Frederick Taylor). Let us equally recall that Foucault in his study of panopticism in modern society has always linked it to the development of capitalism and observed that it is hardly surprising that prisons resemble factories, which in turn resemble prisons.[21]

Finally, none of the existing works actually discusses the functioning of capitalism and how modern surveillance may have affected it. The logic implied in the arguments of those who use the notion of 'surveillance capitalism' may be summarized as follows: corporations increasingly collect and share various types of data; because data is then monetized - used by corporations to make profit - it therefore means that we are dealing with 'surveillance capitalism'. Thus, for example, Priya Kumar, in her analysis of corporate privacy policies changes, draws on the work of Zuboff and argues that the privacy policy changes in question "offer evidence that suggests several of the world's largest internet companies operate according to the logic surveillance capitalism".[22] This is so, according to the author, because companies "then employ advanced data analysis techniques to determine how to use [the obtained data] to extract revenue from advertisers, transforming the data into what Zuboff calls 'surveillance assets'".[23] A similar claim is made by Jacob Silverman in his analysis of the impact of corporate surveillance on individual privacy when he argues that "personal information and behavioral tracking have emerged as major assets in today's surveillance capitalism".[24] In other words, in such works the term 'surveillance' is attached to the term 'capitalism' simply because the former involves data collection, while one of the characteristics of the latter is profit-making; because data is gathered by corporations for the purposes of profit-making, they end up with the notion of 'surveillance capitalism' (which, in addition, remains unexplained because none of these authors actually clarifies what they mean by 'surveillance capitalism', with the exception of Zuboff's reference to 'information capitalism' quoted above). There is no attempt to discuss issues such as the share of data-based businesses in overall economic activity, or the relationship of data gathering and monetization with traditional factors of production, or the impact of data and data-based processes of value creation upon more conventional industries and production processes.

This paper proceeds differently. It agrees with the assertion that in the current phase of capitalism surveillance plays an important role in capital accumulation, and that we are dealing with an important qualitative change in this mode

of production. But the reasons for this are different from the ones given by the authors examined above. It is argued here that the changes that capitalism is undergoing have to do with the emergence of new means of production which may be called 'the means of connection', namely digital platforms, and which allow their owners to create surplus value. As we will see below, some platforms perform this *independently* (they are referred to here as 'independent means of production'), while others *participate* in the process of value creation in combination with other means of production such as physical capital and human labour - these platforms may be called 'auxiliary means of production'. Thus, it will further be argued that alongside financial capital and industrial capital we are now witnessing the rise of 'platform capital' which is beginning to play an important role in capital accumulation (but not (yet) to such an extent as to allow us to speak of 'platform capitalism' as does Nick Srnicek[25]). The *modus operandi* of this 'platform capital' consists in continuous data collection, analysis and monetization in one way or another; to put it differently the basis of the functioning of digital platforms is constant information gathering with respect to users (and increasingly material objects as well), its sorting, profiling, cross-referencing and ultimately employment in the process of value creation. Just as traditional industries require more raw materials to expand, platforms too depend for their operation and growth on the raw material that they use, namely, data. In other words, the tendency to invade or violate individual privacy is *structural* and may not be reduced to intentions and actions of individual actors (e.g., Google, as in the case of Zuboff's analysis, or Facebook, or Amazon or any other platform); as a matter of fact, platform capital only becomes capital when it can access data, which, in turn, has become a commodity. In this respect it will also be argued that data may now be added to Karl Polanyi's list of three 'fictitious commodities',[26] that is, the ones that are not produced for sale but become saleable in capitalism - land, labour and money. And just as Polanyi maintained that the commodification of labour or land threatened the existence of society and the environment, it will be suggested that the increasing commodification of personal data has implications not only for human dignity, but for different kinds of individual rights and for the existence of democratic politics more generally. Overall, the paper concludes that we now live not in a period of 'surveillance capitalism', but of the rise to prominence (and, in the not-so-distant future, perhaps even dominance) of 'platform capital' in global capitalism. Because, as mentioned above, its ability to create value depends on surveillance, surveillance is the DNA of platform capital.

Returning to the case of Cambridge Analytica, what this implies is that it is necessary to go far beyond the study of the mechanisms that allowed this data theft (the app used, the manner in which it obtained user data, the lack of oversight on the part of Facebook, the interests of Cambridge Analytica, etc.). What is required is to place this event into the framework of analysis of more fundamental or structural conditions that render such cases possible. And these structural conditions have to do with the *modus operandi* of platform capital, which has resulted in massive accumulation of data on different categories of users by platforms such as Facebook. In this context, different actors, both governmental and non-governmental, may naturally be tempted to get access to this data for various purposes. Thus, state security services may be interested in this data to track criminals or terrorist suspects. Data brokers, such as Acxiom, Experian or PeekYou, which collect information about individuals from different public and private sources (census, driving records, court reports, voter registration, health care authorities, etc.) also use different platforms (Facebook, Twitter, LinkedIn and others) to enrich their databases (and they also sell to these platforms the information on their users that the latter do not possess). Consultancies and different actors such as political parties, elections candidates or incumbent officials that they work with are similarly eager to know as much as possible about their target populations (e.g., particular groups of voters). In other words, cases of access to user information without their consent, such as the National Security Agency's collection of data from various sources (including platforms) revealed by Edward Snowden in 2013, or in the case of Cambridge Analytica at present, happen because user data keeps on being accumulated and sorted by platform capital, which is totally dependent on it for its operation. But, even if data thefts by third parties might be minimized, using better regulations and oversight, so far as digital platforms continue to function, individual privacy, in one way or another, will continue to be invaded and violated; even if data protection and privacy regulations are reinforced, platforms will continue to attempt to bypass them, simply because they have to. In this respect, those who have mobilized against Cambridge Analytica but have not questioned the practice of 'overt' or 'legitimate' data collection and monetization, may be said to be unintentionally contributing to the further normalization of surveillance practices adopted by platform capital and its partners, thereby to serving their interests.

The paper is structured as follows: the first section examines the growth of digital platforms in recent years, the key aspects of their functioning and the manner in which these 'cloud-based' means of connection become independent means of production, or combine with traditional means of production, to create value. The second section discusses

the centrality of ever expanding surveillance to the operation of platforms which necessitates constant profiling and sorting, evaluation and ranking, notation and monitoring and then returns to the case of Cambridge Analytica.

Section 1: The Rise of Platform Capital

The last decade or so has been marked by the growth of digital platforms and their total dominance in some economic sectors (e.g., internet search and social networking) and a growing importance in others (e.g., urban transport). Now, what exactly are platforms? In simple terms, they may be described as digital infrastructures that connect producers, consumers, service providers, advertisers and other groups in an interactive ecosystem and enable the exchange of goods, services or information.

The development of platforms has been spectacular: today, the top 4 enterprises in Forbes's list of most valuable brands are platforms, as are eleven of the top twenty.[27] Most of recent IPOs and acquisitions have involved platforms, as have most of the major successful startups. The list includes Apple, Google, Microsoft, Facebook, Twitter, Amazon, eBay, Instagram, YouTube, Twitch, Snapchat, WhatsApp, Waze, Uber, Lyft, Handy, Airbnb, Pinterest, Square, Social Finance, Kickstarter, and many others. Although most platforms are US-based, they are a really global phenomenon and, as a matter of fact, are now playing an even greater role in developing countries which did not have viable commercial infrastructures at the time of the Internet Revolution and seized the opportunity that it presented to structure their industries around the cyberspace. Thus, in China, for example, many of the most valuable enterprises are platforms, for instance Tencent (owner of the WeChat and QQ messaging platforms) and Baidu (China's search engine); Alibaba controls 80 percent of China's e-commerce market through its Taobao and Tmall platforms, with its Alipay platform being the largest payments platform in China (Moazed and Johnson, 2016).[28]

While at the moment the share of platforms in the overall S&P 500 is not very significant (under 5 percent), they are projected to make up the majority of the top valuations in the S&P 500 within the next five to ten years with the key candidates being LinkedIn, Twitter, Zillow, GrubHub, Uber, Snapchat, Airbnb, Dropbox, and Pinterest whose present valuations already exceed S&P 500 market cap requirements. And if current trends continue, platforms could make up 50 percent of the S&P 500's net income within twenty-five years.[29]

The importance of platforms is also attested by the number of users (often numbered in millions and, in some cases, even in billions as in the case of Facebook which, in the first quarter of 2018, had more than 2 billion active users[30] (statista.com)) regularly connecting to their various cloud-based services, as well as by the wide range of sectors they now operate. Thus, to name the key sectors, platforms are now central in internet search (Google, Yahoo, Bing); social networking (Facebook, LinkedIn, Instagram, Snapchat); internet auctions and retail (eBay, Taobao, Amazon, Alibaba); on-line financial and human resource functions (Workday, Upwork, Elance, TaskRabbit), urban transportation (Uber, Lyft, Zipcar, BlaBlaCar), tourism (Kayak, Trivago, Airbnb), mobile payment (Square Order, PayPal, Apple Pay, Google Wallet); and software development (Apple's App Store, Google Play Store, Windows App store) and mobile health or mHealth (23andMe, PatientsLikeMe, Parkinson mPower). Platform-based solutions are also currently being adopted in more traditional sectors, such as industrial production (GE, Siemens), agriculture (John Deere, Monsanto) and even clean energy (Sungevity, SolarCity, EnerNOC).

These developments have not gone unnoticed and a large number of new terms have been developed in academic and non-academic literature in an attempt to conceptualize this novel phenomenon. However, upon a closer examination, it may be observed that these terms, and the analyses that are carried out by those who use them, tend to focus on different *specific* innovations and novelties rather than on more structural transformations that capitalism is undergoing with the rise of platforms. For instance, those who use a now very popular term 'sharing economy' (also 'peer-to-peer economy' or 'collaborative economy'), discuss the rise of collaborative consumption, renting and bartering;[31] those who speak of 'gig economy' focus mostly on the new possibilities offered by platforms for hiring independent contractors and freelancers, instead of full-time employees, and the implications of this for labour;[32] finally, the authors employing the term 'on-demand economy' tend to highlight the 'convenience of delivery' offered by platforms to consumers, particularly in sectors such as restaurant industry, grocery purchases and deliveries as well as transportation, as well as on issues related to labour rights.[33]

There do exist, however, several studies that have attempted to go further than that to view these developments as signaling fundamental changes in the nature of capital accumulation and in capitalism as a socio-economic system. One notable work in this respect is Nick Srnicek's *Platform Capitalism* mentioned earlier in which the author examines the rise of platform businesses as part of the historical trajectory of capitalism and links it in particular with the crises of the 1970s and 2008. This work provides many rich insights into the nature of platform-based businesses (and a very useful typology of platforms which this paper will utilize in the discussion of platforms below), but the author seems to overstate the case for 'platform capitalism' because, as indicated above, the share of platform-based enterprises and activities in total production, even in the United States, remains relatively small (at least for now).

Now, Srnicek identifies the following types of platforms: advertising platforms, cloud platforms, industrial platforms, product platforms and lean platforms. In the light of the argument developed above, I would suggest that we can distinguish between (1) platforms as means of production in their own right, that is, the ones that generate revenue using data as raw material without combining with other factors of production, and (2) platforms as means of production which are used with other factors of production to create value.

In the first category - platforms as independent means of production - we may include what Srnicek refers to as 'advertising platforms', as well as the ones that I would call 'barter platforms'. The former generate most of the revenue from targeted advertising and generally operate as follows: they collect data from users (and increasingly from connected objects), and then use different algorithms to process this 'raw material' and fabricate products that are sold to advertisers, namely the possibility to target specific categories of users, sorted according to various criteria (their tastes, interests, income, age-groups, preferred leisure activities, hobbies, etc.). All the inputs (with the exception of servers) as well as the products in this case are immaterial or 'cloud-based' (made available to users via the internet from providers' servers), such as algorithms, lines of code, advert spaces for targeting user profiles, and so on.

The leading platform in terms of total revenue from targeted advertisement is Google, a company that was established in 1996. Google started by collecting data from user searches in order to improve search results. In 2000, Google launched AdWords and began to sell space to advertisers for targeted advertisement through an automated auction system. The revenues that Google has been able to generate using this service have quickly grown very significantly: for example, in 2017, Google and its numerous affiliates (YouTube, Applied Semantics, DoubleClick, etc.) generated 95.38 billion US dollars in advertisement revenue out of the total Google's revenue of 110,9 billion that year (i.e., 86% of the total).[34] Revenues of other platforms providing internet search are much lower, but nevertheless substantial. Thus, in 2016 Yahoo earned 4.66 billion US dollars from advertisement, while Bing's ad revenues in the same year amounted to 1.6 billion US dollars.[35] The share of profit from targeted advertising is even greater in the case of Facebook, which, with over 1.5 billion subscribers has possibly become the world's largest media company without producing a single piece of original content. In 2017, it earned 39.94 billion US dollars in ad revenues which amounted to as much as 98 percent of Facebook's global revenue.[36]

The business model of barter models is based on providing a 'cloud-based' market place for buyers and sellers of goods. In the case of eBay, the revenue comes mostly from fees that the platform charges for each transaction, but in recent years it has started making profits from targeted advertising as well. Thus, in 2017, the total revenue of eBay amounted to 9.56 billion US dollars, most of it from marketplace transaction fees with advertisement revenues amounting to 897 million (9.3% of the total).[37] By contrast, Taobao, the Chinese equivalent of eBay, does not charge its sellers neither a listing fee nor cut of sales. It makes its money from targeted advertising.

As regards the second category - platforms as auxiliary means of production - it comprises platforms which provide tools for others to use, that is, to create products created additional inputs and means of production are required. They are much more numerous and operate in wide range of sectors. To begin with, there are what Srnicek calls 'cloud platforms', that is, those that provide different 'cloud-based' tools that may be employed by users to create and market their own products or services. For example, developers may use Apple's ecosystem (XCode and the iOS SDK) to build apps and sell them via Apple's App Store, for which Apple will take a cut from each sale. In other words, developers use their own means of production (i.e., computers) and their human capital (i.e., programming skills), which are combined with the tools offered by platforms to create the final product. Exactly the same model is used by Microsoft and Google which offer similar tools for developers to create apps. The place where the apps are sold depends on the platform whose tools each developer choses (App Store, if the platform

chosen was Apple; Google Play if it is Google's Android-based tools, or Microsoft App store in the case of Microsoft tools).

We may also include in this category those platforms that allow sellers of different services to find customers. One of the main examples here is Uber, a taxi service which was launched in San Francisco in March 2009. Five years later it operated in more than 200 global cities and was valued at more than $50 billion, and all this without owning a single car. All Uber does is produce transactions using its platform (drawing on traffic data and the locations of drivers and riders) between drivers, who own their means of production (cars and their labour) and riders, charging drivers a fee. The same applies to Airbnb, in whose case the suppliers of services (accommodation) own the houses and apartments that they let to travelers and pay Airbnb a fee. Those platforms that help 'independent contractors' as they call them, such as freelancers as well as service providers offering services such as house repair or house cleaning, find customers. Such platforms are now numerous with some of the key examples being TaskRAbbit, UpWork, Workday or Elance.

Another type of platform that may be included in this category is Amazon Web Services (AWS), a platform initially built for managing Amazon's logistics but which quickly became used by Amazon as a cloud computing service rented to other users, producers or sellers who require on-demand software development tools, services for servers, storage and computing power, operating systems, and ready-made applications. As Srnicek observes, the utility of this practice for other businesses is that they do not need to spend the time and money to build up their own hardware system, their own software development kit, or their own applications. They can simply rent these on an 'as needed' basis. The comparison of this service to electricity provision, made by Amazon's CEO Jeff Bezos,[38] is indeed valid: just as centralized electricity provided on-demand replaced individual generators that early factories employed, Amazon now provides a centralized digital infrastructure which more and more industries require at a certain stage of the production process. Following Amazon's success in this field (AWS reached an estimated worth of around $70 billion in 2015[39]), Microsoft also started providing other businesses with an artificial intelligence platform, which enables them to build their own bots ('intelligence as a service'), while Google started selling its cloud-based machine-learning processes. Chinese Alibaba is also moving into the provision of different of similar cloud-based services.

Finally, we may mention here what Srnicek labels 'industrial platforms' and this is the latest development in platform business. Here, digital platforms begin to participate in traditional manufacturing processes via the installation of sensors and trackers in different components or inputs connected to the internet, the process known as 'Industry 4.0' or as the 'fourth industrial revolution',[40] after steam power, electricity and assembly lines, and computerization. The aim of those involved in Industry 4.0 is to create 'smart factories' based on systems of real-time sharing of information by individual elements involved in the production about their location or state with other components or with human laborers or managers. One of the first platforms built for industries is MindSphere of Siemens, a cloud-based operating system whose development cost Siemens 4 billion US dollars and which connects products, plants, systems, and machines. In addition to its own apps, Siemens allows third party app producers, to build apps and market them via MindSphere (i.e., in exactly the same way as Apple's App Store or Google's Google Play operate with app developers). A number of third party apps are already available at MindSphere, such as, for example, Manufacturing Sustainability app and Production Confirmation app developed by Atos, Assembly Line Self Optimizing App by Evosoft or Connected Asset Management by Accenture.[41] Another major Industry 4.0 platform is Predix which has been developed by General Electric which offers two development environments: full stack developers with skills building microservices oriented apps may access Predix Platform building blocks in its full stack and high control environment, while coding novices may take advantage of the low code, high productivity environment of Predix Studio for rapid app development.[42] In 2015, the European Commission also launched a research project into Industry 4.0 whose objective is to provide Cloud-based Rapid Elastic Manufacturing (CREMA) based on the EaaS (Everything as a service) cloud computing and innovative use of Artificial Intelligence and semantic technologies. The primary purpose of the project to help industries increase efficiency of manufacturing through an on-demand leasing and releasing of manufacturing assets on a pay-per-use basis.

Now, having seen the examples of the manner in which digital platforms operate, either as independent or auxiliary factors of production, we may return to the issue of the relationship between surveillance and digital platforms, which is the subject of the next section.

Section 2: Surveillance: the DNA of Digital Platforms

The central element common to all the different types of digital platforms examined in the previous section is that they involve the ownership of mostly 'cloud-based' or immaterial assets (such as algorithms or lines of codes), with very little ownership of physical capital (except servers). From their point of view, as mentioned in the *Introduction*, the process of capital accumulation is based virtually exclusively on 'the new oil', namely data, which is collected, processed, analyzed and eventually monetized in one way or another. Without this 'raw material', their business model cannot exist. Marx, in volume I of *Capital* observed with respect to capital that it only comes to life when it meets in the market place "a special commodity" - labour-power;[43] capital, he argued, "arises only when the owner of the means of production and subsistence finds the free worker available, on the market, as the seller of his own labour-power".[44] We may paraphrase Marx and state that for platform capital to come to life it needs to meet another very special commodity - user data.

And it may be argued that this new commodity could be added to Karl Polanyi's list of three fictitious commodities, that is, the ones that are not produced for sale but become saleable in capitalism - land, labour and money: "labor, land, and money are obviously *not* commodities; the postulate that anything that is bought and sold must have been produced for sale is emphatically untrue in regard to them. [...] Labor is only another name for a human activity which goes with life itself, which in its turn is not produced for sale but for entirely different reasons, nor can that activity be detached from the rest of life, be stored or mobilized; land is only another name for nature, which is not produced by man; actual money, finally, is merely a token of purchasing power which, as a rule, is not produced at all, but comes into being through the mechanism of banking or state finance. ... The commodity description of labor, land, and money is entirely fictitious".[45] User data is perhaps the most fictitious of all because not only is it not produced for sale by users (who simply browse the internet or share content with friends on social media), but it is also the most immaterial of all; it is a 'cloud-based' fictitious commodity.

Now, what is crucial to observe here is that Polanyi, particularly with respect to his argument about human labour and land becoming saleable commodities under capitalism, sought the emphasize the risks that this involved for the society and the environment. Thus, he argued that "to allow the market mechanism to be sole director of the fate of human beings and their natural environment, indeed, even of the amount and use of purchasing power, would result in the demolition of society".[46] In disposing of a man's labor power the system would "dispose of the physical, psychological, and moral entity 'man' attached to that tag".[47] And nature "would be reduced to its elements, neighborhoods and landscapes defiled, rivers polluted, military safety jeopardized, the power to produce food and raw materials destroyed". As regards the practice of personal data collection and monetization, what we are dealing with is a major threat to the right to privacy which, in turn, is one of the most fundamental human rights as its violation not only undermines human dignity but can also compromise the exercise of several other individual freedoms, such as freedom of expression, freedom of press, freedom of thought, conscience and religion, freedom of assembly and association, as well as a number of socio-economic rights (particularly labour rights).[48] It is for this reason that the growing disregard for the right to privacy, especially in Western societies, has been designated by Giorgio Agamben as one of the main threats to the very existence of democratic politics in our time.[49] In this respect it may be argued that the commodification of personal data and its incessant collection, which is the basis for the capacity of a growing number of business actors to massive profits, has far-reaching implications for Western democracies. Let us now take a closer look at the manner in which different kinds of platforms engage in surveillance practices to gather the data that they require for their operation.

The capacity to acquire data on individual users is absolutely crucial for platforms operating as independent factors of production. It is their 'raw material', it is what they need to generate revenue, and this explains the extent of user information that they collect and store. Thus, the examples of user data that Google gathers include: user location from the first day of using Google on a smart phone; search history across all of the user's devices (retained by Google even if deleted by the user); information on every app and extension used (places and frequency of usage of the app, persons or entities communicated with using the app, etc.); all of the user's YouTube history; all bookmarks, emails, contacts, Google Drive files, products bought through Google; finally, many other pieces of information that may be gathered from a smartphone (music listened to, photos taken, books purchased, phones owned, pages shared, number of steps walked per day). The extent of Facebook's data collection is equally impressive: every message or file sent or received by the user; all the contacts in the user's phone; pages or media liked, commented and shared; every log into Facebook (where the user logged in from, at what time, and from what kind of device); all the stickers ever sent on Facebook; all the apps ever connected to the user's Facebook account;

the location metadata inside photos, and even what is seen through the camera in its apps (for instance, when members use filters or masks); user phone's attributes such as battery level, signal strength and available storage.

To acquire more data, platforms such as Google and Facebook have been increasing their capacity of data gathering both *in breadth* and *in depth*. The former involves augmenting the number of sources from which data is mined: the acquisition of other established companies or promising start-ups and the creation of links to other databases and networks. Facebook, for instance, has expanded the breadth of its data mining capability by acquiring companies such as Instagram and WhatsApp, and by combining the information obtained from these companies with data gathered from various data brokers. Thus, Facebook has for years collaborated with data brokers such as Acxiom Corp and Experian to create better advertisement targets for certain categories of advertisers (automakers, luxury goods producers and consumer packaged goods companies, who do not sell directly to consumers and have relatively little information about who their customers are.[50] Google has bought companies such as YouTube, DoubleClick, AdMob, HTC, and others to similarly combine data from wider variety of sources. As regards the depth of data acquisition, this involves developing new tools to know more about users within the existing platform (e.g., capacities to better geolocate users, to improve the methods of analysis of their online activities, such as measuring the time they spend consulting certain types of material, the number of consultations per day, etc.). And, ultimately, they require constant improvement of their means of analysis (algorithms) of the data obtained to develop more nuanced profiles and clusters of users in order to ameliorate the final products that they can sell to advertisers as the latter seek improved 'conversion rates', that is, the percentage of users who end up purchasing their goods or services following ads placed on these digital platforms. Thus, Google modifies its search algorithm around 500–600 times a year to improve its data analysis capacities and provide better search results. Most of these changes are usually minor, but Google from time to time Google introduces important algorithmic updates (such as Google Panda and Google Penguin).

As regards those platforms that function as auxiliary means of production, the extent of their dependence on data may vary but they all share the same imperative to improve their capacity of data gathering and analysis. For example, platforms that provide tools and the market place for developers to create and sell apps (Google Play, Microsoft App Store or Apple App Store), need to know more about the customers who purchase specific types of apps in order to improve their targeted advertisement methods and thereby increase the sales of apps from which they take a cut. Online stores such as Amazon or Alibaba, or barter platforms such as eBay or Taobao, also have the same imperative. Platforms such as Uber or those that bring together freelancers and customers, need to know as much as possible about the performance of drivers, cleaners or repairers. To achieve this, more sophisticated techniques of, for instance, driver tracking, are developed (e.g., Uber now constantly monitors the position of drivers to minimize waiting times for customers) and the performance of each driver or 'independent contractor' is incessantly rated.

Such imperatives are less significant in the case of industrial platforms, but let us recall that Industry 4.0 is not only about developing real-time communication systems among material components of the production process, but also among objects *and* human laborers. This creates an incentive to also equip workers with sensors and other electronic devices, which in turn will allow the evaluation of their performance as well. As a matter of fact, such employee monitoring and tracking devices are already widely used in different sectors. Thus, companies such as Sociometric Solutions have developed employee ID badges (equipped with microphone, location sensor and accelerometer) to monitor who employees talk to, in what tone of voice and for how long.[51] Similar monitoring techniques are developed by many other companies (InterGuard, ObserveIt, Steelcase, Epicenter, etc.). Epicenter has gone as far as developing microchips that are implanted under the worker skin which allows not only monitoring of employees, but which enables workers to use these chips to open doors, buy snacks from vending machines or operate printers. More recently Amazon patented a wristband that tracks warehouse workers' movements and can vibrate to point an employee's hand in the right direction.[52] In the light of these developments it is highly likely that such devices will, sooner or later, be employed by Industry 4.0 platforms as well, and more personal data will thus be mined and analyzed.

Now, one of the key obstacles that digital platforms face in their quest to acquire more and more 'raw material', that is, to know more and more about users, workers and 'independent contractors is, of course, different regulations that exist to protect user privacy and which are embodied in different national and international legal instruments. The main means that platforms use to bypass this obstacle is obtaining user consent - user acceptance of Terms of Service (ToS) (and this, in fact, is the central difference between digital platforms such as Facebook, Google or

Amazon and the case of Cambridge Analytica). However, do users really know what they sign up for? It is plausible to suggest that this is not the case as far as the dominant majority of users are concerned because ToS, as a rule, are characterized by high complexity, unintelligibility and unreasonable length, and provisions concerning user permission to gather and analyze user data, and to share it with third parties, are very hard for common users to identify and understand. Thus, for example, it took 8 hours and 59 minutes for an actor hired by the consumer group 'Choice' to read 73,198 words of Amazon Kindle's terms and conditions.[53] In cases where there is a possibility to turn off certain functionalities to better protect privacy, upon installation or initial registration such functionalities are turned on by default and it takes some effort to find out how to disable them. For example, Microsoft's Windows 10 operating system has 16 different sub-menus for privacy options, all of which are enabled by default upon installation (location, programs installed and all the information concerning their usage, access to webcam and microphone, access to contacts, e-mails, calendar, files downloaded, photos and videos, music, search history and browsing history). All these tricks to keep users unaware of what exactly they sign up for when they join different platforms are not due to legal complexities involved or omissions on the part of platforms; it is their business model that pushes them to invent such methods to bypass the obstacles that may prevent them from getting more and more of their main 'raw material'.

In this respect we can see that the difference between the methods of digital platforms and those employed by Cambridge Analytica are not fundamentally different. Yet, it is the latter's action that has led to public outrage, although the data that it gathered is a drop in the ocean compared to the amount of information that platform capital routinely collects in order to reproduce and valorize itself. The implications of this, to which we may now turn, are important.

First, protesters and critics who targeted Cambridge Analytica *de facto* condemned only covert measures of data collection, and indirectly contributed to the normalization of the ones for which users give their 'consent' by accepting various ToS. Second, if platforms are allowed to continue to operate, structural conditions that render possible covert data acquisitions or thefts (i.e., attempts to acquire data possessed by platforms without user consent) will remain. Indeed, platforms such as Facebook (with over 2 billion active users, as mentioned above) amass gigantic amounts of data on user tastes, interests, political beliefs, habits, travel, - and so on, and those who require such data for different purposes, be they state- or non-state actors, will have an incentive to get access to it. Third, even though the public outcry results has resulted in the collapse of Cambridge Analytica, there remain other similar consulting groups (e.g., i360, Data Trust, etc.) which benefit from trade with digital platforms (selling to platforms the information on their users that they do not possess, and acquiring from them information that they can monetize in one way or another) and which hold increasingly large amounts of data. Thus, Data Trust, for instance, is currently able to collect over 1800 pieces of information about individuals including things like the last time a person downloaded porn or ordered Chinese food.[54] In short, so long as digital platforms are allowed to operate, routine privacy invasions, indispensable for the operation of platform capital, will continue, and the conditions for more 'covert' attempts to get access to data possessed by platforms on the part of other actors will remain. And, so long as platform capital exists, the idea that data is a commodity and that its possession may generate revenue, will become more and more objectified and naturalized, which in turn threatens not only individual privacy and human dignity, but also a whole range of other individual liberties, and with them, democratic politics in general.

Conclusion

The preceding analysis allows us to draw a number of general conclusions. To begin with, as regards the current phase of capitalism, the position taken here is different from the one advanced by Shoshana Zuboff that we live in the period of 'surveillance capitalism; it is also different from those who, like Nick Srnicek, believe that we live in the era of 'platform capitalism'. It is argued here that modern-day capitalism is characterized by an increasing importance of platform capital, which is a specific type of capital because for its reproduction and valorization it depends on an immaterial 'raw material' - data. In other words, data is the commodity that platform capital needs to meet in the market place in order to become platform capital, to paraphrase Marx once more. What this means, as we have seen above, is that surveillance - the collection and sorting of data on individuals (and increasingly material objects as well) - is an indispensable instrument that digital platforms and their partners must continuously employ in order to operate. Such an imperative is particularly pronounced for those types of platforms that we have referred to here as 'independent means of production' (such as internet search engines or social networks which use mostly immaterial factors of production such as algorithms and data). However, we have seen that those platforms that act as 'auxiliary means of production' (those that provide app developers with programming and marketing tools, or

those that allow drivers or accommodation providers to find customers, as in the case of Uber or Airbnb, and even those platforms that are involved in Industry 4.0) also face the necessity to constantly improve their capacity to collect and process data.

In this context, as was argued above, data has become a commodity - it is something that may now be bought and sold in order to generate profit in one way or another. It is a new kind of Polanyi's 'fictitious commodities': not only is it not produced for sale as the other three (users surfing the net and chatting on social media do not generate data in order to sell it), but it is also totally immaterial. The commodification of personal data, as the commodification of human labour or land discussed by Polanyi, has significant social implications: as argued above, what we are dealing with is a major threat to the right to individual privacy which is one of the most fundamental human rights for it is indispensable for the exercise of different other individual rights, such as freedom of expression, freedom of press, freedom of thought, conscience and religion, freedom of assembly and association, as well as a number of socio-economic rights. Following Agamben, it was suggested that rendering personal data a 'fictitious commodity' threatens the very existence of democratic politics.

Concerning the case of Cambridge Analytica, with which this paper started, the main argument consisted in showing that it is only a tip of the iceberg. The extent of the data acquired by Cambridge Analytica is dwarfed by the likes of Google, Facebook, and other types of platforms examined above, which routinely collect, analyze and monetize the information about individuals. As argued above, the only difference between Cambridge Analytica and such routine personal data collection is that the former used more covert means to get access to it; however, when one examines ToS of most platforms it is plausible to argue that most users are equally unaware about the manner in which data about them is gathered by platforms and the 'consent' that they give by signing ToS can hardly be seen as an informed consent. In this respect this paper has made several claims with respect to public outrage that followed the revelations concerning Cambridge Analytica: first, that those who focused on Cambridge Analytica *de facto* denounced only such 'covert' measures of data collection, and thereby contributed to the normalization of the ones for which users give their 'consent' by signing ToS; second, allowing digital platforms to continue to operate, structural conditions that make attempts to steal data from platforms will remain and similar scandals (involving either public or private actors) are likely to happen again; third, even though the public outcry led to the collapse of Cambridge Analytica, there remain other data brokers and consulting groups (e.g., i360, Data Trust, etc.) which benefit from trade with digital platforms and which hold more and more data.

Now, there are, of course, activists who do see overt data collection as problematic (most notably, civil society organizations such as Privacy International, Electronic Foundation Frontier or Tactical Technology Collective) and who call for better protections of individual privacy. There are also attempts by policymakers to introduce more stringent privacy rules, such as the EU's General Data Protection Regulation (GDPR), which comes into force on May 25, 2018. However, because of the growing share of platform capital in capitalism, putting in place any major obstacles to its operation will inevitably produce negative impact on economic growth. Thus, for example in the European Union privacy protection regulations are significantly stronger than in the United States. As a result, the "number of billion-dollar startups in the US is forty-two, but only thirteen in the EU. ... Recent evidence suggests that this EU data privacy regime is already having a notable economic impact".[55] Peter Thiel, PayPal co-founder, for example, recently stated that there were no successful tech companies in Europe because of stricter regulations.[56] In this respect, it is plausible to suggest that there certainly will be more opponents of any stronger privacy protections for this reason as well. In short, it is thus important to understand that if citizens wish to regain control over data that concerns their private lives, they must organize to challenge platform capital as a whole, and not just 'covert' data acquisitions by individual actors such as Cambridge Analytica. However, it is also important to realize that the struggle that awaits them will be long and very difficult.

Notes

[1] Cadwalladr, Carole, and Emma Graham-Harrison. "Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Mata Breach." *The Observer*, March 17 mars, 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[2] Rosenberg, Matthew, Nicholas Confessore, and Emma Cadwalladr. "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.
[3] Solon, Olivia. "Facebook Says Cambridge Analytica May Have Gained 37m More Users' Data." *The Guardian*, April 4, 2018. https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought.
[4] The Guardian. "Cambridge Analytica Whistleblower: 'We Spent $1m Harvesting Millions of Facebook Profiles'." March 17, 2018. https://www.youtube.com/watch?time_continue=63&v=FXdYSQ6nu-M.
[5] Cadwalladr and Graham-Harrison, "Revealed."
[6] Tajani, Antonio. A Tweeter Message, posted on March 19. https://twitter.com/EP_President/status/975683240777453569.
[7] Brito, Ricardo. "Brazil Prosecutors Open Investigation into Cambridge Analytica." *Reuters*, March 21, 2018. https://www.reuters.com/article/us-facebook-cambridge-analytica-brazil/brazil-prosecutors-open-investigation-into-cambridge-analytica-idUSKBN1GX35A.
[8] Wootliff, Raoul. "Israel to Probe Facebook over Cambridge Analytica Data Breach." *The Times of Israel*, March 22, 2018. https://www.timesofisrael.com/israel-to-probe-facebook-over-cambridge-analytica-data-breach/.
[9] CA Commercial. "Cambridge Analytica and SCL Elections Commence Insolvency Proceedings and Release Results of Independent Investigation into Recent Allegations", London, May 2, 2018. https://ca-commercial.com/news/cambridge-analytica-and-scl-elections-commence-insolvency-proceedings-and-release-results-3.
[10] Manokha, Ivan. "Cambridge Analytica's Closure is a Pyrrhic Victory for Data Privacy', *The Conversation*, May 3, 2018. https://theconversation.com/cambridge-analyticas-closure-is-a-pyrrhic-victory-for-data-privacy-96034; also, Manokha, Ivan. "La disparition de Cambridge Analytica, une victoire à la Pyrrhus', *Le Monde*, May 18, http://www.lemonde.fr/idees/article/2018/05/17/cambridge-analytica-pour-regagner-le-controle-des-donnees-les-citoyens-doivent-remettre-en-cause-le-systeme-dans-son-ensemble_5300517_3232.html.
[11] Foster, John Bellamy, and Robert McChesney. "Surveillance Capitalism Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age." *Monthly Review* 66 (2014) (digital version). https://monthlyreview.org/2014/07/01/surveillance-capitalism/.
[12] Zuboff, Shoshana, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30 (2015): 75-89; and Zuboff, Shoshana. "The Secrets of Surveillance Capitalism." *Frankfurter Allgemeine Zeitung*, March 5, 2016. http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html.
[13] Zuboff, "Big Other," 76-77.
[14] Zuboff, "Big Other," 75.
[15] Baran, Paul and Paul Sweezy. *Monopoly Capital* (New York, Monthly Review Press, 1966).
[16] Foster and McChesney, "Surveillance Capitalism."
[17] See, for example, Weber, Max. *Economy and Society*, *Volume I* (Berkeley, University of California Press, 1978); Giddens, Anthony. *The Nation-State and Violence: A Contemporary Critique of Historical Materialism*, *Volume II* (Cambridge, Polity Press, 1985); Dandeker, Christopher. *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day* (Cambridge: Polity Press, 1990).
[18] Zuboff, "Big Other," 81-82.
[19] Zuboff, "Big Other," 82.
[20] See Wood, Ellen. *Democracy Against Capitalism: Renewing Historical Materialism* (Cambridge, Cambridge University Press, 1995); Wood, Ellen. *The Origin of Capitalism* (London: Verso, 2002); Brenner, Robert. "The Origins of Capitalist Development. A Critique of Neo-Smithian Marxism," *New Left Review*, 104 (1977).
[21] For example, Foucault, Michel. *Surveiller et punir. Naissance de la prison* (Paris: Gallimard, 1975); Foucault, Michel. "The Eye of Power" in Gordon, Colin. (ed.) *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977* (New York, Pantheon Books, 1980).
[22] Kumar, Priya. "Corporate Privacy Policy Changes during PRISM and the Rise of Surveillance Capitalism." *Media and Communication* 5 (2017) 68.
[23] Kumar, "Corporate Privacy," 68.
[24] Silverman, Jacob, "Privacy under Surveillance Capitalism." *Social Research: An International Quarterly* 84 (2017) 147.
[25] Srnicek, Nick. *Platform Capitalism* (Cambridge: Polity Press, 2017).

[26] Polanyi, Karl. *The Great Transformation: The Political and Economic Origins of Our Time* (New York, Farrar & Rinehart, 1944).
[27] Forbes. "The World's Most Valuable Brands: 2017 Ranking." 2017. https://www.forbes.com/powerful-brands/list/.
[28] Moazed, Alex, and Nicholas Johnson. *Modern Monopolies: What It Takes To Dominate The 21st-Century Economy* (New York: St. Martin's Press, 2016).
[29] Moazed and Johnson, *Modern Monopolies.*
[30] Statista.com
[31] For example, Brescia, Raymond. "Regulating the Sharing Economy: New and Old Insights into an Oversight Regime for the Peer-to-Peer economy." *Nebraska Law Review* 95 (2016); Juho Hamari, Mimmi Sjöklint and Antti Ukkonen. "The Sharing Economy: Why People Participate in Collaborative Consumption." *Journal of the Association for Information Science and Technology* 67 (2016); Taeihagh, Araz. "Crowdsourcing, Sharing Economies and Development." *Journal of Developing Societies* 33 (2017).
[32] For example, Todolí-Signes, Adrián. "The End of the Subordinate Worker? Collaborative Economy, On-Demand Economy, Gig Economy, and the Crowdworkers' Need for Protection." *International Journal of Comparative Labour Law and Industrial Relations* 33 (2017): De Stefano, Valerio. "The Rise of the 'Just-in-Time' Workforce: On-Demand Work, Crowd Work and Labour Protection in the "Gig-Economy." *ILO Conditions of Work and Employment Series* 71 (2016); Stewart, Andrew, and Jim Stanford, J. "Regulating Work in the Gig Economy: What are the Options?" *The Economic and Labour Relations Review* 28 (2017).
[33] For example, Heller, Nathan. "Is the Gig Economy Working?" *The New Yorker*, May 15, 2017. https://www.newyorker.com/magazine/2017/05/15/is-the-gig-economy-working; Natour, Faris. "Respecting Human Rights in the On-Demand Economy: Closing the New Governance Gap." *Business and Human Rights Journal* 1-2 (2016).
[34] Statista.com
[35] Statista.com
[36] Statista.com
[37] Statista.com
[38] Quoted in Srnicek, *Platform Capitalism*, 79.
[39] Asay, Matt. "Amazon's Cloud Business is Worth at least $70 Billion." *ReadWrite*, October 23, 2015. https://readwrite.com/2015/10/23/aws-amazon-cloud/.
[40] Marr, Bernard. "Why Everyone Must Get Ready for the 4th Industrial Revolution." *Forbes*, April 5, 2016. https://www.forbes.com/sites/bernardmarr/2016/04/05/why-everyone-must-get-ready-for-4th-industrial-revolution/#4d63d373f90b.
[41] Siemens.com
[42] Ge.com.
[43] Marx, Karl. *Capital: Critique of Political Economy*, *Volume I* (London: Penguin Books, 1976) 270.
[44] Marx, *Capital*, 274.
[45] Polanyi, *Great Transformation,* 75-76, original italics.
[46] Polanyi, *Great Transformation,* 76.
[47] Polanyi, *Great Transformation,* 76.
[48] See, in particular, Westin, Alan. *Privacy and Freedom* (New York, Atheneum, 1967); Rule, James. *Private Lives and Public Surveillance: Social Control in the Computer Age* (London, Allen Lane, 1973); Bauman, Zygmunt; Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and Rob Walker. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8 (2014): 121-144; Bennett, Colin. "Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications." *Surveillance & Society* 13 (2015): 370-384; Ball, Kirstie. "Workplace Surveillance: an Overview." *Labour History* 51 (2010): 87-106; Boghosian, Heidi. *Spying on Democracy: Government Surveillance, Corporate Power, and Public Resistance* (San Francisco: City Lights Books, 2013); Manokha, Ivan. "Why the Rise of Wearable Tech to Monitor Employees Is Worrying", *The Conversation*, January 3. https://theconversation.com/why-the-rise-of-wearable-tech-to-monitor-employees-is-worrying-70719; Foer, Franklin. *World Without Mind: The Existential Threat of Big Data* (New York: Penguin Press, 2017).
[49] Agamben, Giorgio. "From the State of Control to the Praxis of Destituent Power", *Roar Magazine,* February 4, 2014. https://roarmag.org/essays/agamben-destituent-power-democracy/.

[50] Reuters. "Facebook Cuts Ties to Data Brokers in Blow to Targeted Ads." *Business News*, March 28, 2018. https://www.reuters.com/article/us-facebook-privacy/facebook-cuts-ties-to-data-brokers-in-blow-to-targeted-ads-idUSKBN1H41KV.
[51] Manokha, "Why the Rise".
[52] The Guardian. "Amazon Patents Wristband that Tracks Warehouse Workers' Movements." February 1, 2018. https://www.theguardian.com/technology/2018/jan/31/amazon-warehouse-wristband-tracking.
[53] Choice. "How Long Does It Take to Read Amazon Kindle's Terms and Conditions?" March 17, 2017. https://www.youtube.com/watch?v=sxygkyskucA.
[54] Palast, Greg. "Cambridge Analytica is Not Alone: i360 and Data Trust Disastrous for Democracy." *TheRealNews.com*, March 29, 2018. https://therealnews.com/stories/cambridge-analytica-is-not-alone-i360-and-data-trust-disastrous-for-democracy.
[55] Geoffrey Parker, Marshall Van Alstyne, and Sangeet Paul Choudary. *Platform Revolution: How Networked Markets Are Transforming The Economy - And How To Make Them Work For You* (New York: W.W. Norton & Company, 2016). Goldfarb, Avi, and Catherine Tucker. « Privacy Regulation and Online Advertising », *Management Science* 57 (2011).
[56] Solon, Olivia. "Peter Thiel: Europe is cracking down on Silicon Valley out of 'jealousy'." *The Guardian*, March 15, 2018. https://www.theguardian.com/technology/2018/mar/15/peter-thiel-silicon-valley-europe-regulation/.