Journal of Intellectual Property Rights
Vol 23, March-May 2018, pp 70-85

Competition and Consumer Privacy in the Cyberspace Market

Joseph A Klien[1], PM Rao[2] and Manoj Dalvi[2†]

[1] Fisher Broyles LLP, 445 Park Avenue, Ninth floor, New York -10022, USA

[2]Long Island University, CW Post Campus, 720 Northern Blvd, Greenvale, New York - 11548, USA

Received: 18 September 2017; accepted: 10 August 2018

This paper will examine legal and marketing implications of certain Internet technological developments impacting competition and consumer protection in cyberspace. The paper will explore to what extent antitrust and consumer protection laws are adequate to deal with the challenges to a competitive marketplace and consumer privacy posed by the development of cyberspace technologies and markets, for example, Internet search engines, social networks and wearable devices. The paper concludes that legal tools for protecting a competitive cyberspace marketplace are fairly robust, while the legal tools to protect consumers from being tracked and profiled by marketers and from the potential intrusions of individual privacy made possible by even more advanced Internet connected sensor and related data-based technologies are still a work in progress. At the same time, the extent of further government regulation in this area must be carefully balanced so as not to unduly restrict data dependent innovation.

Keywords: Consumer privacy, cyber security, economics, exclusivity, social media networking, *Google*, *Facebook*, *Apple*, Internet usage,Header should be Klie EU Commission, public policymakers, digital marketing, consumer privacy protection, Competition Commission of India, U.S. Antitrust Law, United States Federal Trade Commission

The economics of social media platforms is built on two strategies: Obtaining more users, and then increasing the amount of personal information collected about those users that can be turned into targeted ads; and getting users to spend increasing amounts of time on these platforms so they can see more ads. This paper examines the legal and marketing implications of certain Internet technological developments impacting competition and consumer protection in cyberspace. It explores the extent to which antitrust and consumer protection laws are adequate to deal with the challenges to a competitive marketplace and consumer privacy posed by the development of cyberspace technologies and markets like Internet search engines, social networks and wearable devices. The paper provides in detail the growth of Internet technology and analyzes the risk to a competitive markets place from *Google; Facebook*; as well as issues of cyber security and consumer privacy protection. The paper concludes that the legal tools for protecting a competitive cyberspace marketplace are fairly robust, while the legal tools to protect consumers from being tracked and profiled by marketers and from the potential intrusions of individual privacy made possible by even more advanced Internet connected sensor and related data-based technologies are still a work in progress.

Growth of Internet Technology

The Internet has operated on the principle of "*if you build it, people will come*." The Internet's phenomenal growth has spawned "*network effects*", a positive demand-side externality in which the value of a product or service to an individual user rises as the number of users increase.

"An industry platform with network effects leads to more users to adopt the platform, which in turn leads to more users and complementors."[1] The worldwide growth of internet users between 2000 and 2017 was over 933% (Table 1).[2]

From its origin in U.S. Government sponsored research in the mid 1980's, the Internet and the World Wide Web that it supports, have grown exponentially in usage. The Internet is now moving into a new

†Corresponding Author: Email:Manoj.Dalvi@liu.edu

Table 1 — World Internet usage and population statistics (25 March 2017 – Update)

World regions	Population	Population % of world	Internet users	Penetration rate (% Pop.)	Growth 2000-2017	Users % table
Africa	1,246,504,865	16.6 %	345,676,501	27.7 %	7,557.2%	9.3 %
Asia	4,148,177,672	55.2 %	1,873,856,654	45.2 %	1,539.4%	50.2 %
Europe	822,710,362	10.9 %	636,971,824	77.4 %	506.1%	17.1 %
Latin America/ Caribbean	647,604,645	8.6 %	385,919,382	59.6 %	2,035.8%	10.3 %
Middle East	250,327,574	3.3 %	141,931,765	56.7 %	4,220.9%	3.8 %
North America	363,224,006	4.8 %	320,068,243	88.1 %	196.1%	8.6 %
Oceania/Australia	40,479,846	0.5 %	27,549,054	68.1 %	261.5%	0.7 %
Total	7,519,028,970	100 %	3,731,973,423	49.6 %	933.8%	100 %

significant phase of its evolution. This phase of Internet technology is referred to by Internet experts as the Internet of Things ("IoT").[3] that has been defined as "a world of networked smart devices equipped with sensors and radio-frequency identification, connected to the Internet, all sharing information with each other without human intervention."[4] It is "a decentralized network of 'smart' objects — items that can sense, log, interpret and communicate information, and act on their own accord or in cooperation with other objects. Their computing power and connectivity may range from very limited to extensive. The smart objects may sense information generated within themselves or from the external world. And they may communicate with other objects, with computers or with people. One way to visualize the "IoT" is to think of the Internet as a network connecting computers and people, then add to it a proliferation of sensors and actuators (mechanical devices that move something) embedded in physical objects and connected to the network."[5] Credit Suisse IT Hardware Analyst Kulbinder Garcha has predicted that "the market for wearable technology will increase tenfold to as much as 50 billion US dollars" by 2018.[6] Gartner has predicted more generally that there will be nearly 26 billion devices on the "IoT" by 2020.[7]

In the "initial stages of the "IoT", identity is provided to selected objects and the value to users here comes from the interaction of these identities with other intelligent systems, such as, smart phones or web services."[8] In the "intermediary stage, the 'things' in the "IoT" develop the ability to sense their surroundings, including the environment, location, and other devices. Value to users here comes from those things taking action based on that information.[9] In the "final stage of maturity for the 'IoT', technology availability, capacity, and standardization will have reached a level that doesn't require another device (such as a smart phone or web service) to function. Not only will the 'things' be able to sense context, but they will be able to autonomously interact with other things, sensors, and services.[10] The *Apple* Watch is a current example of "IoT", in the form of a wearable device. Wearables, like the *Apple* Watch, can track information about a person (*via* skin contact), the location (GPS), the activity, and an individuals' vital signs.

The Internet of things technology continues to develop[11] and open up new markets along an arc that will enable some of the most personal information about online users, sensed from *things* (for example, wearable devices or sensors connected to the outside or even inside our bodies) and the Internet. The user data is exchanged online with other *things* connected to the Internet, which will act upon the user data they receive automatically without any human intervention or direct knowledge. The sheer volume of data generated by the devices[12] gives rise to serious privacy questions. The data generation creates a point of entry to hackers, allows companies to gather information about your habits,[13] or even invade your home.[14] The challenge, therefore is to bake both privacy and security into interconnected devices, thereby protecting the individuals who use them.

Risks to A Competitive Marketplace and Consumer Protection

Competitive Market

In the "information economy" where the focus has been on the presence of significant supply-side economies of we now focus on the demand side as well. Thus, consumers place greater emphasis on large networks than smaller ones. "The utility that a subscriber derives from a communications service increases as others join the service"[15] and its value to

a user, therefore, depends on how many other users there are. This phenomenon is known as network effects or external demand-side economies.[16]

Since the Internet at its base is a communications network; network effects are magnified and have helped drive the exponential growth of the Internet. Network effects have also operated to provide first mover advantages to certain online firms which have successfully developed and deployed disruptive technologies. If those firms' market power in the product and geographical markets in which they operate, defined as the relevant markets in which to measure the extent of such power for antitrust purposes, results from their innovations and superior products and services, consumers benefit.

US case law is unambiguous that there is no automatic violation of antitrust law (or competition law as this area of law is sometimes referred to outside of the United States) merely because of legitimately obtained monopoly or dominant market power as a result of innovation or business acumen.[17] Particularly under U.S. Law dealing with the antitrust offense of monopolization,[18] firms with monopoly power in a relevant market (defined for antitrust purposes both in terms of products and geography) engage in illegal monopolization only if they abuse that power by engaging in anti-competitive behavior.[19] In Europe, there is a somewhat lower market share threshold for establishing a presumption of firm *dominance* in a relevant market than exists under U.S. Antitrust Law.[20] In India, the Competition Commission of India defined "a dominant position is linked to the concept of market power which allows an enterprise to act independently of competitive constraints. Such independence enables an enterprise to manipulate the relevant market in its favour to the economic detriment of its competitors and consumers."[21] Thus, despite some differences of nuance at the margins, there is substantial overlap between the U.S and Europe as well as other non-U.S. jurisdictions like India in the kinds of acts that can constitute abuse of substantial market power (whether called monopolization as in the United States or abuse of market dominance as in non-U.S. jurisdictions such as Europe). These include exclusionary agreements, product bundling or tying requirements,[22] predatory pricing, or refusal to provide competitors with vital information or access to an essential facility or a network that is necessary in order to be able to compete on the merits.

The Case of *Google*

Google and *Facebook* are prime examples of high technology firms that have built up critical masses of users in their respective search engine and social network markets. As a result they have amassed substantial market power in those markets.[23] Even in fast-changing and dynamic Internet-based markets such as those involving search engines and social networks, the antitrust/competition law analytical framework and tools that have been applied in more traditional markets under the Sherman Act or its non-U.S. analogues remain useful. To be sure, there are more challenges in defining the relevant markets for both search engine and social network products and services. There are also reasonable concerns about the ability of regulators and courts in emerging high technology markets to correctly analyze the effects on competition of an alleged anti-competitive practice, as balanced against a valid efficiency-enhancing business justification for such a practice that cannot be as readily achieved in a less restrictive manner. Courts and regulators must be able to distinguish between firms with substantial market power that are simply reaping the legitimate commercial rewards of successful innovation versus firms exploiting the substantial market power that such innovations make possible to unfairly foreclose competition. But such concerns should not be blown out of proportion. Antitrust and competition law cases in the recent past involving firms in other high-tech markets, such as Microsoft in the operating software and browser space, can provide guidance for regulators and courts in examining comparable scenarios in the search engine and social network spaces.

For example, consider *Google*. Once *Google* achieved dominance in the search engine market, over a 90% share in the entire European Union[24], it was in a position to potentially leverage its dominant power over Internet searching to the detriment of competitors in search-dependent online advertising markets.

Competitors have charged that *Google* was manipulating search results from consumers' use of its search engine in favor of displaying products or services in advertisements or shopping sites from which *Google* commercially benefited. The *Google* search can be a general web search or a thematic search. Its share of the searches and the other sites as of October 2015 is given in Fig. 1.[25]

This built-in favoritism in the display of search results, competitors and antitrust regulators have

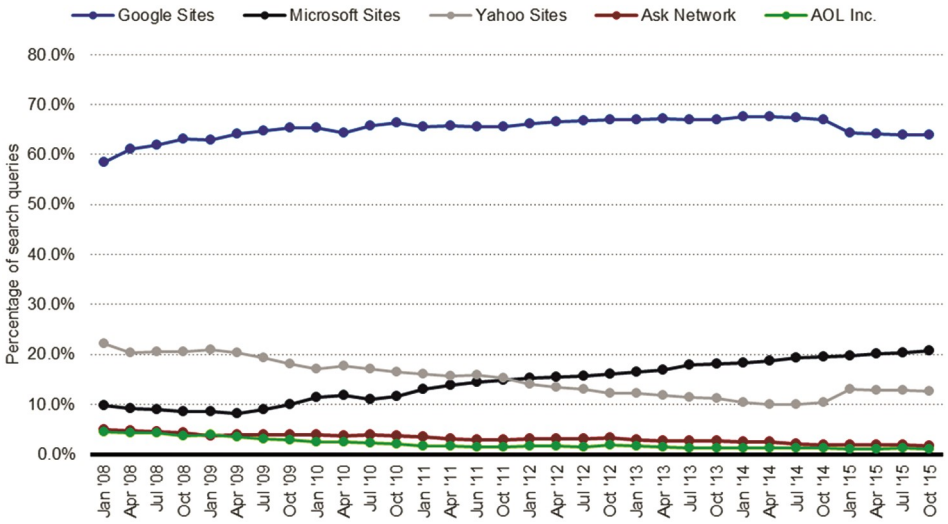

Fig. 1 — Percentage of queries for selected search engines, January 2008 to October 2015

charged, created significant barriers to entry for rival advertisers and shopping sites attempting to compete with *Google* in search-dependent online advertising markets. Moreover, *Google's* addition of value-added free features such as *Google* Maps and *Google News* to its search engine platform can raise barriers to entry for competitors in both the search engine market and markets for products that compete with those value-added features offered by *Google*.

> "*Each time new features are incorporated into existing dominant platform software, less integrated competitors are harmed. Consumers are also potentially harmed as well by the diminution of choice and the possible exclusion of better options*."[26]

An antitrust analysis of *Google's* alleged anti-competitive practices would proceed along the lines of what is the relevant market, and how it would be analyzed? A search engine arguably possessing the extent of network externalities that *Google's* search engine displays may be viewed as an essential facility, which cannot be used unfairly to leverage control over the search engine facility to obtain market power in a competitive market dependent on access to the facility such as online ads.[27] However, it can be argued that *Google's* market is not the more typical one-sided market that is analyzed under antitrust law. *Google* has two sets of consumers: the searchers and the advertisers. It is a two sided market, where searches are free and no switching costs are incurred to use another search engine. *Google*, therefore, must provide search results that are useful to the searchers to prevent them from switching to another search engine. Nevertheless, *Google's* established brand advantage and much larger search content than its smaller competitors may keep many loyal consumers from switching. Moreover, *Google* search gets better as more people use it, as a result of refinements in its search-results algorithm that in turn have adversely affected specialized search sites such as *Yelp* in the past. Thus, *Google's* potential to leverage market power resulting from its search-results algorithm and established brand advantages that maintain a huge loyal customer base would require careful antitrust analysis.

The EU Investigation

The antitrust investigation of *Google*, which started in 2010, by the European Commission responsible for Competition Policy (EU Commission) represents the most intensive such investigation to date. The EU Commission listed four areas of particular concern in a 2012 press release[28]

Favoritism in Display

In its general search results, *Google* displays links to its own vertical search services differently than it does for links to competitors. We are concerned that this may result in preferential treatment compared to those of competing services, which may be hurt as a consequence. Vertical search services refer to specialized search engines which focus on specific topics, such as for example restaurants, news or products.

Misappropriation of Competitive Data

Google may be copying original material from the websites of its competitors such as user reviews and

using that material on its own sites without their prior authorization. In this way they are appropriating the benefits of the investments of competitors.

Exclusivity

Google and partners on the websites for which *Google* delivers search advertisements (i.e., advertisements that are displayed alongside search results when a user types a query in a website's search box) have entered into agreements that "result in de facto exclusivity requiring them to obtain all or most of their requirements of search advertisements from *Google*, thus shutting out competing providers of search advertising intermediation services."

Restrictions on Ad Campaign Portability

Google has placed restrictions on the portability of online search advertising campaigns from its platform *AdWords* to the platforms of competitors. *Google* imposes contractual restrictions on software developers which prevent them from offering tools that allow the seamless transfer of search advertising campaigns across *AdWords* and other platforms for search advertising.

In February 2014, *Google* and the EU Commission reached a tentative settlement in which *Google* committed that "whenever it promotes its own specialised search services on its web page (e.g. for products, hotels, restaurants, etc.), the services of three rivals, selected through an objective method, will also be displayed in a way that is clearly visible to users and comparable to the way in which *Google* displays its own services."[29] *Google* also had previously agreed to other concessions dealing with the EU Commission's concerns – for example, to remove exclusivity requirements in its agreements with publishers for the provision of search advertisements and to remove restrictions on the ability for search advertising campaigns to be run on competing search advertising platforms.[29]

However, after receiving more complaints from some of *Google*'s competitors, the EU Commission decided to reopen the proceeding and seek more concessions from *Google*.[30] In July 2016 the EU Commission decided to initiate new proceedings against *Google*.[31]

On 27 June 2017, the European Commission fined *Google* €2.42 billion for breaching EU antitrust rules. It held that "*Google* has abused its market dominance as a search engine by giving an illegal advantage to another *Google* product, its comparison shopping service."[32] The company was ordered to cease its activities within 90 days or face penalties of 5% of the average daily worldwide turnover of *Alphabet*, *Google*'s parent company.[32]

Although Europe has led the way in pursuing antitrust investigations into *Google*'s behavior, it has not done so alone. The United States Federal Trade Commission (FTC) launched its own antitrust investigation into *Google*'s alleged abuse of its substantial market power in the Internet search industry. *Google*'s share of the search engine market in the United States is less than its share of the European market, but it still was measured as a 67.6% market share as of April 2014,[33] remained constant in October 2015[33] and in 2016.[34]

The FTC turned out to be not as aggressive as the EU Commission in pursuing *Google* for possible antitrust violations, arguably due in part to *Google*'s lower share of the search engine market in the United States *vis a vis* Europe.[35] The FTC announced a settlement in 2013 with *Google*, in which *Google* agreed to a number of concessions, including the easing of access by its competitors "to patents on critical standardized technologies needed to make popular devices such as smart phones, laptop and tablet computers, and gaming consoles."[36] *Google* also agreed, along lines similar to its initial settlement with the EU Commission, "to give online advertisers more flexibility to simultaneously manage ad campaigns on *Google*'s *AdWords* platform and on rival ad platforms; and to refrain from misappropriating online content from so-called 'vertical' websites that focus on specific categories such as shopping or travel for use in its own vertical offerings."[36] However, the FTC appeared to shy away from any detailed analysis as to whether *Google*'s vertical integration of its own content (e.g., maps, shopping comparisons, flight search results) into its organic search results —'search bias'—foreclosed competitors from access to Internet users, resulting in anticompetitive harm.[37]

Thus, while the EU Commission has decided to press on with its investigation and possible antitrust enforcement at the urging of *Google*'s competitors, the FTC determined that with regard to "the specific allegations that the company biased its search results to hurt competition, the evidence collected to date did not justify legal action."[37] The FTC emphasized in its statement announcing its settlement that its focus was on protecting competition, not individual competitors.

Outside counsel hired by the FTC for its investigation concluded that the "evidence did not demonstrate that *Google*'s actions in this area stifled competition in violation of US Law."[37] Other investigations of *Google*'s alleged abuse of its market power have been launched around the world from Latin America to Asia.

The Indian Investigation

Consim Info Private Limited, matrimonial search engine, and The Consumer Unity and Trust Society (CUTS) urged[38] the Competition Commission of India (CCI) to investigate the potential anticompetitive conduct of *Google* in the Indian e-commerce market and online advertising and related markets. They argued that "*Google* runs its core business of online search and search advertising in a discriminatory manner, causing harm to advertisers and indirectly to consumers and creating an uneven playing field by favoring its own services and of its vertical partners, by manipulating the search algorithms."[39]

The online search market in India consists of two kinds of participants: The search engines in the world markets like *Bing, Altavista* and *Google*; and the Indian search engines, *Guruji, 123* and *Khoj*. The Indian search engines seem to cater to a rather different market and are of a very different quality. Language is an important factor in the "search" market in India. Not all the users want to conduct their search in the same language.

The Commission, after perusing the record and hearing the arguments, found that there was a *prima facie* case to direct the Director General (DG) to cause an investigation to be made into the matter.[40] Their concern was that *Google* used its dominance in the search engine/online advertising markets to affect the growth of online shopping and online travel markets. Accordingly, the Commission by its order dated 3 April 2012 directed the DG to investigate the matter and to submit its report.

The Director General said [41,42]

> "*Google is found to be indulging in practices of search bias and by doing so it causes harm to its competitors as well as users. Investigation has revealed that Google integrates / blends its own specialised / vertical search services/options/features/features in its online general web search services in universal results and commercial units using mechanisms that do not apply in an equivalent manner to non Google websites / web content.*
>
> *Therefore, Google conduct is found to be anti competitive in terms of Section 4(2)(a)(i), 4(2)(b)(ii), 4(2)(c) and 4(2)(e) of the Act."*[43]

The potential liability faced by *Google* if the Competition Commission of India rules against it is the imposition a fine of 10% of its annual sales[44] or it could break up *Google* into independent entities.[45] The Commission, by its Order of 8 February 2018[46] penalized *Google* for "infringing antitrust conduct" and imposed a penalty of Rs135.86 crore ($21 million) translating to 5% of the firm's average total revenue generated from different business segments of its India operations for the financial years 2013, 2014 and 2015.

The Case of *Facebook*

The original concept of *Facebook* was that it was a social networking site; competing with other sites like *Friendster* and *MySpace*.[47] These social networks, too had substantial network effects. According to the former *Facebook* President, Sean Parker, *Facebook* dominated because "*Facebook* entered the market through college and the reason we went in through college was that college kids were generally not *Myspace* users. College kids were generally not *Friendster* users."[48]

Facebook's social network passed 1.19 billion monthly active users worldwide as of September 2013, an increase of 18% year-over-year, dwarfing all rivals. In Q4 2015 the number of monthly active users was 1.6 billion users.[49]

Facebook's mobile monthly active users alone were 874 million as of September 30, 2013, an increase of 45% year-over-year.[50] Figure 2 shows that the number of monthly mobile active users exceeded 1.4 billion users in Q4 2015.

Compared to the more relatively mature search engine market, currently dominated by *Google*, the social networking market is still developing. *Google* has used its time-saving, bottom-of-funnel advantage to become, by a wide margin, the richest company in mobile advertising. *Google* controls over 40% of the small-screen ad market, a lead that is padded with the company's dominance in search advertising.[20] If you remove search and focus exclusively on display ads (banners and video, but not search), it's *Facebook* that controls more than a third of the market. That's three times more than *Google*'s share and five times more than Twitter.[32]

Facebook is an engine of consumer surplus, but, unlike *Google*, it earns its prodigious income by

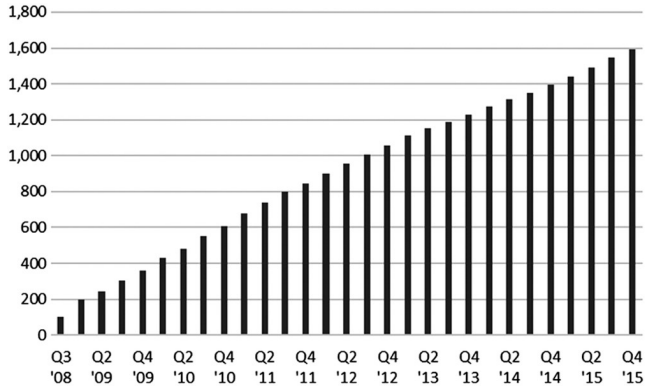

Fig. 2 — Number of monthly active *Facebook* users worldwide Q3 2008 to Q4 2015 (in millions)

monetizing time spent, rather than time saved. *Facebook*'s huge number of users provides a well-spring of user data which it can use to enable target advertising and allow favored applications developers access to the data. However, to the extent that network effects also apply to social networks such as *Facebook*, the result may be the creation of frontal entry barriers for new entrants that do not have access to the large base of users and data regarding the users that a firmly established firm in the marketplace such as *Facebook* already possesses.

Facebook has a major competitive advantage over rival social networking sites that do not have access to such wealth of user data. The number of users and the array of fine-grained information that users have posted are on a scale vastly superior to its competitors.[51] Moreover, people who rely on *Facebook* for communications and connections with multiple users – friends, family, colleagues, etc. – are reluctant to terminate their participation in *Facebook* or to rely on an alternative social network site with far fewer users. This contributes to the stickiness of the system.

As a result of the combination of the network effects and stickiness of *Facebook*'s social network system, there is a serious possibility that *Facebook* already has market power over current users who are, or feel, locked-in to the system.[26] Knowledge is power. *Facebook* controls myriad bits of personalized information about its user base that it can organize, synthesize, analyze and manipulate to create individual profiles valuable to online advertisers and applications developers using such data for their own commercial benefit. As more applications developers become part of *Facebook*'s ecosystem, benefiting from and adding value to the social network platform because of what they can do with the data controlled by *Facebook* that does not exist in such quantities or formats on other social network platforms, *Facebook*'s social network attracts even more users. This in turn attracts more and more online advertising at the expense of *Facebook*'s competition. *Facebook* stated in its report of second quarter 2014 results that its revenue from advertising was $2.68 billion in the second quarter, a 67% increase from the same quarter in 2013. Mobile advertising revenue represented approximately 62% of advertising revenue for the second quarter of 2014, up from approximately 41% of advertising revenue in the second quarter of 2013.[52]

Facebook still faces competition from apps like *Snapchat*. *Snapchat*, an app for sending disappearing messages, has evolved from a teen phenomenon into a mainstream media platform. It relies on advertising to users who watch videos compiled by its staff and those from media brands. The huge leap forward for *YouTube* was UGC (user generated content) but this emerged into new stars, new ways of producing content and new ways of consuming it. Similarly, *Snapchat* has messaging (like *WhatsApp, WeChat*) but also has 'stories' (a day in the life of a user or media brand) and 'discover' which is where short-form, professionally produced media exists. *Snapchat*'s ability to innovate is the future of social media and at the very initial stages of this app we can not only glimpse into the future but also have a sense of the product quality of Snapchat and the competition it should pose for *Facebook*.

While the market for social networking may be somewhat difficult to define with precision for antitrust purposes, measurements centered on comparative user populations on sites that have at least some social networking attributes, such as the total number page views or the number of registered users, may be helpful. When measured in this fashion, *Facebook* appears to be on the cusp of market power,[26]– perhaps as high as the 60% range, depending on what firms are included in determining market share. The more locked in to *Facebook* its users believe they are, the narrower the relevant market is in terms of interchangeability with alternative social network sites. If digital display advertising revenues are used as the appropriate market share measure instead, *Facebook*'s market share may be only in the 20% range, again depending on what firms are included in the calculations.[53]

Reaching a judgment as to whether a firm has monopoly or dominant market power is the first step

in determining whether the offense of monopolization or abuse of dominance exists or not. It is noted that there is little in the way of current case law or enforcement actions to provide guidance on what acts cross the line separating legitimate and anti-competitive activities.[54] We are also dealing primarily with access to user information rather than to something more tangible such as hardware or software.

It can be argued that the network effects on social networks create strong barriers to frontal competition; but not to lateral competition.[26] A niche social network can evolve into something bigger, and network effects will not matter.[55] For example, *Twitter* adopted the 'Status Update' feature of *Facebook*; and *Instagram* its photo sharing feature. In both these cases there was a gateway to the other network, where there is no need to have all of your contacts, just the ones you interact with the most. *Twitter* and *Instagram* have built alternative communities centered on a specific feature: comments and picture sharing.

If the FTC's and the EU Commission's disparate dispositions of their investigation of alleged *Google* anti-competitive conduct is any indication, we can expect a more aggressive stance by the EU Commission than the FTC with respect to *Facebook*. Once dominance is established, theories of liability are more robust in the European Union. These include theories of bundling, predatory pricing, denial of access to essential facilities, and a general duty of a dominant firm not to abuse its dominance, which are unknown, or much more narrowly interpreted, in modern U.S. antitrust law.[55]

In sum, although effective legal tools exist within the body of antitrust and competition law and regulations to deal with anti-competitive conduct of online firms such as *Google* and *Facebook*, they also face completion. Nevertheless, regulators and courts must remain vigilant for signs of anti-competitive conduct and must be willing to be creative in their use of the legal tools available to prevent or remedy harm to competition that may result if such conduct remains unchecked.

Consumer Privacy Protection

Adopted by more than 2.5 billion people in the first 20 years of its existence, the Internet permeates through every aspect of our personal lives. Moreover, the unprecedented demand for mobile devices further convolutes legal issues when it comes to Internet use and what is private and public information. One cannot pick up a newspaper, watch TV, listen to the radio, without some direct or veiled reference to the lack of information security or intrusions into personal privacy. Every day it seems that more and more systems are breached and more and more personal information is made available either on the web or, worse, the dark web (link is external).

In this milieu *Facebook* (and others) makes money off the data collected through advertising revenue, generating $40 billion in revenue in 2017, with about 98% coming from advertising across *Facebook* and *Instagram*. Significant data collection is also occurring at *Google*, *Twitter*, *Apple*, and *Amazon*.[56] These companies continually expand their products and services enabling endless opportunities to collect increasing amounts of information on their customers. The tradeoff for the American consumer is to provide more personal data, in exchange for free or very low cost products and services. The potential for further growth and innovation based on the collection of data is limitless. However, the potential for abuse is also significant.[57]

This data gathering has ignited a discussion on the future of data privacy in our society. Consumers do not understand how their data is collected, protected, transferred, used and abused. Furthermore, a rapid convergence in the data mining, algorithmic and granular analytics capabilities of companies like *Cambridge Analytica* and *Facebook* is creating powerful, unregulated and opaque 'intelligence platforms'.[58] These have an enormous impact on our behavior, including what we buy, what we learn and even how we vote and underscore the importance of protecting consumer privacy.

Social Networking sites

Data portability and data scraping are a concern particularly on social networking sites.[59] *Facebook*, for example, prohibits third party users from copying their data[60] but allows its own users to copy their own information as a backup or move it to another site.[61] Despite this prohibition, *Cambridge Analytica* obtained *Facebook*'s data for use in the Trump Presidential Campaign.[62]

Portability of data, however, allows taking data to a different venue and evade the privacy restrictions imposed by the original site.[1,63] But as *Facebook* faces the inexorable public company pressure of increasing usage and revenues quarter after quarter without end, it undoubtedly will have to look at more creative and

aggressive ways to access, process, and monetize our personal information. For example, the real value of Whatsapp that was acquired by *Facebook* is the number of text messages processed by it daily.[64] By accumulating user data in an anonymous way *Facebook* can improve ad targeting before the text message is deleted.

Tracking by Websites

Consumers using the Internet benefit from the wealth of free information available on websites and the ease of purchases and other transactions that e-commerce makes possible. But in availing themselves of what the Internet offers consumers, they leave behind a trail of their pattern of usage.[65] Marketers, including brokers of marketing information to online advertisers, have utilized software tools to track, collect and analyze website visitors' interests and preferences. They glean users' data from tracking of their web surfing and other patterns of usage.

On the plus side, the gathering of information by so-called *first party trackers* on how an individual uses a particular site can enable the website owner to improve the user's direct interaction with that site during future visits. The gathering of individuals' usage data regarding their sessions on the websites where the users being tracked have initiated the sessions themselves will enable such users to take advantage of its features such as auto-complete forms and shopping carts for purchases. As long as the website discloses that information regarding the user's interaction with the site is being collected by the site for subsequent commercial use, the user has a choice as to whether he or she is willing to share certain information in exchange for the services offered by the site.[66]

With appropriate privacy policies in place that are implemented, including a prominently placed notice to allow consumers to make an informed choice as to whether or not to accept the conditions of utilizing the site, there is adequate protection for consumers in such instances. More problems arise, however, when so-called *third party trackers* collect data on consumer web views and usage across the Internet.[67] The purpose of such tracking is not to help consumers more efficiently navigate a particular website with which they have consciously chosen to initiate a session. Rather, the purpose is to literally follow consumers around the Internet without their knowledge and surreptitiously build a detailed profile of each consumer based on everything the consumer does while on the Internet, which can be sold to advertisers to enable targeted advertising.[68] A majority of Internet users do not know they are being tracked on the Internet so extensively in real -time, nor do they have any idea where the detailed dossier put together from the tracking about their interests, preferences, and the like ends up.[68]

Privacy Laws

To date, privacy laws have not been fully capable of controlling the negative impact on consumer privacy caused by the proliferation of tracking technologies used for consumer profiling and online advertising purposes. Individuals continually contribute to the collection of data as they participate in a digital economy, such as shopping online, using *Google* or even posting on *Facebook*. The data that is collected poses privacy risk in three dimensions: age, period and frequency.[69]

The European Union has tried to make some headway with its Directive 2009/136/EC (EU 2009 Directive),[70] which, among other things, was aimed at curbing the placement of cookies (text files that allow websites to recognize their users) and other tracking mechanisms on users' computers without the users' informed consent, unless they are strictly necessary for delivery of a service requested by the user, such as an online shopping cart.[71] The EU 2009 Directive, which each member state is supposed to incorporate in its national legislation, was intended to apply not only to cookies as they exist today but also to future technological means for companies to track online users' preferences. Yet, Tracking Walls and Take -It-Or-Leave-It Choices offers consumers little choice but to click '*I Agree*' to tracking.[71]

The EU collectively[72] and individual European member states have taken some actions to control the use of consumers' online data, without their knowledge or consent, for the purpose of creating consumer profiles. For example, a German privacy regulator ordered *Google* to seek an explicit and informed consent of the respective user before *Google* takes such data to create online user profiles.[73] The following is an excerpt from the German regulator's September 30, 2014 press release:

> *According to the view of the data protection authority the ongoing practice of user profiling affects the privacy of Google users far beyond the admissible degree. Google is ordered to take the necessary technical and organizational measures to guarantee that their users can*

decide on their own if and to what extend their data is used for profiling. Google Inc. collects substantial information about the habits of their users. Many use the various services provided by the company in their daily life on a regular and extensive basis. This includes those registered with Google (e.g. users of Gmail and most owners of Android phones) as well as those that use Google services (like the search engine) without being logged on. The content and usage data collected thereby reveal a lot about the individual and his or her interests, habits and ways of life… For such an extensive profiling that combines all data there is no justification in either German national or European law. Therefore, such processing is only lawful given an explicit and informed consent of the respective user or, in so far the laws provide for that, the possibility for the user to object.[74]

National regulators in France,[75] Italy[76] and Spain[77] have challenged *Google* on similar grounds. Other European countries are also considering challenges, but time will tell how effective they will be.[78] More recently the European Parliament passed the General Data Protection Regulation (GDPR) in 2016. Its provisions, that go into effect on 2 May 2018, is an ambitious set of rules spanning from requirements to notify regulators about data breaches to transparency for users about the data being collected and the purpose of the collection. For example, the rules protect data related to basic identity; location; IP address; cookie data; RFID tags; health and genetic data; racial or ethnic data' political opinions; and sexual orientation.[79]

As an example of a country outside of the United States and Europe, Brazil has one of the largest domestic Internets in the world. Its regulators have directed their attention to online user data privacy issues. The Consumer Protection and Defense Department of Brazil fined Brazil's largest telecommunications company in July 2014 for failing to notify internet users that their browsing activities had been tracked and sold to third-party advertisers.[80] Brazil is also one of the countries that has expressed the most public concern at its highest government level regarding the sharing of its citizens' Internet data by U.S. online firms such as *Google* with the U.S. National Security Agency. For that reason, it is seeking to restrict the storage of its citizens' user data by *Google*, *Facebook* and other multinational online platform providers to data centers within Brazil.[81]

Although 85% of U.S. online consumers oppose Internet ad tracking, according to Consumer Reports,[81] U.S. Law has lagged behind in effectively prescribing or restricting such behavior. While there are no specific legal requirements as of yet in the United States comparable to the European and Brazilian models discussed above, the FTC has recommended policies and best practices which it has urged businesses to consider implementing in connection with their collection and use of consumer data from Internet tracking technologies.[80]

Media, advertising agencies, marketing associations, search engine companies led by *Google*, telecommunications companies such as AT&T and Verizon, and technology companies such as Microsoft, have responded to the FTC's challenge with a voluntary program that amounts to self-regulation. The decision of such firms to forego certain commercial benefits to themselves from customer tracking information in favor of minimizing tracking technology's social costs to individual privacy is not an altruistic one. This choice is driven in part by marketing strategists' concerns with negative impacts on firm-wide reputation and branding.[80]

Under the program, users can click on an icon and be taken to a full disclosure page and an opt-out option. However, such a voluntary program, intended to dispel privacy concerns of some Internet users and to avoid new regulations by the Federal Trade Commission on the EU model, can only be truly effective if there is participation by substantially all online parties with access to user online data. That is not yet the case. Prominent consumer-facing websites themselves, as well as leading browser vendors and search engines with whom consumers regularly interact, do have an incentive to take proactive steps to blunt consumer backlash against them as the privacy implications of their role in tracking become more-well known. However, non-consumer-facing developers of tracking software and information aggregators, of whom consumers may know little or nothing about, have little incentive to curb their tracking-enabling activities on their own as long as the activities remain legal and they have a market of advertisers interested in the results they are able to track and compile.[82]

Recognizing the short-comings of relying entirely on industry self-regulation, the FTC has called for the U.S. Congress to pass comprehensive legislation codifying full protection of consumer privacy rights including the protection of data generated from

consumers' usage of the Internet. In the meantime, the FTC has brought some patchwork enforcement actions pursuant to its current statutory authority, including against *Google* and *Facebook*, requiring them "to obtain consumers' affirmative express consent before materially changing certain of their data practices," and against online advertising networks that failed to honor consumers' wishes to opt out of tracking by advertisers.[83]

Even as the law is still in the process of trying to catch up with regulating Internet tracking and profiling of consumers' user data, Internet of Things technology leapfrogs ahead, posing new challenges to legal protections of consumer privacy. It is projected that by 2015 there were 25 billion connected devices and by 220 there will be 50 Billion devices.[84] The connected devices will enable consumers to remotely access their homes, and regulate their thermostats, or the lights or even warm their dinners. They will enable doctors to manage diseases or connected cars notify first responders in the event of an accident.[85] This increase in connected consumer devices implies that there will be an exponential increase in the average number of daily data capturing consumer activities.

Consider the example of a smart digital watch with wireless capabilities, built-in sensors, and connection to digital networks – perhaps a more advanced version of the *Apple* Watch - that can continuously record an audio and visual record of the wearer's activities streamed to social networks and archived for later retrieval. In this example, not only would the wearer's own personal data such as health-related information be continuously monitored, collected, communicated and processed without the wearer's active involvement. Other people with whom the wearer of the smart digital watch interacts may not be aware that they, too, are being monitored and turned into a data source in real -time for devices or social networks connected to the Internet.

The sheer volume, multiplicity of sources and potential applications of the user data capable of being collected, assembled, analyzed and acted upon through direct connections of devices and other things on the Internet without direct human interaction, let alone knowledge and consent, are staggering.[85] Big Data has a paradox; on the one hand it is beneficial as the data is analyzed;[86] on the other hand, it raises both security and privacy concerns because these networks are inherently insecure and can harm consumers either by accessing their data, attacking the consumer's network or simply by creating safety risks; and it is impossible to make it secure.[87]

The digital footprint left by consumers using the connected devices opens the door to the home of the consumers and that consumers are leaving a digital footprint that opens the door to their online habits and to their shopping habits and their location, and the last thing that is understood is the home, because at the moment, when you shut the door, that is it.[88] The IOT's potential to generate large amounts of personal information has serious implications for consumers. IOT data may reveal an individual's identity, location, medical issues, sexual orientation, socioeconomics or political profile. It might include a live video feed, or report whether doors and windows are locked. And the list goes on.[89] The data could be used in unauthorized ways by unauthorized individuals to systematically bias companies against certain groups that do not or cannot engage in the favorable conduct as much as others or lead to discriminatory practices against protected classes.[90]

Public policymakers differ on the best way to deal with the privacy implications for consumers. Some believe that the notion of privacy in the age of the Internet needs to be fundamentally rethought. Others look first to the private sector to come up with technological solutions and self-regulatory standards of best practices.[91] Still others believe that government action is necessary, although there are serious doubts as to whether the more traditional regulatory mechanisms of notice and consumer consent, including choice of *opt-in* or *opt-out*, would be sufficient in dealing with such fundamentally transformative technologies as the Internet of Things.

For example, in expressing concerns as to whether traditional regulatory tools such as notice would work, the FTC's Director of the Bureau of Consumer Protection, Jessica Rich, said at the end of a daylong 2013 workshop on the Internet of Things that when it comes to the Internet of Things, how can we provide effective notice, particularly with interconnected devices that don't have screens, and when data is being collected passively, perhaps without a consumer's knowledge and added that our next step will not be to propose regulations.[81]

While the FTC is not ruling out regulation in the future, it is relying at present on voluntary private sector actions to deal with the negative externalities imposed on consumers by the Internet of Things. As a

FTC Commissioner said at a 2014 consumer electronics trade show, "It's crucial that companies offering these products that are part of the internet of things act to safeguard the privacy of users to avoid giving the technology a bad name while it is still in its infancy."[92]

Even the European Commission, which has traditionally been a world leader in regulating the use of consumers' online data to protect consumer privacy, has conceded that its current legislative framework on data protection is inadequate to deal with these new challenges.[93] One idea proposed during the FTC's workshop is to encourage companies to build in consumer privacy protections from the very outset. Privacy should be integral to the innovation process with privacy hard-coded in. (FTC, 2012; Page 9) The objective is to take the burden off of consumers to take affirmative steps themselves to signify how they want data about themselves to be treated – which is increasingly impossible for consumers to do in any case because they suffer information asymmetry in terms of how their online data is being used.

Referred to as "privacy by design," innovations could include such features as "defaults or other design features that can help prevent consumers from sharing personal data in an unwanted manner" in the first place. Privacy tools and settings should be as easy to use as the underlying product or service. (FTC, 2012 ; Page 9-10) The development of simplified just-in-time notice and consumer choice options are recommended in this connection. (FTC, 2012, Page 358).

In view of the potential pervasiveness of IoT devices that can collect, communicate and act automatically on users' highly sensitive personal information, firms that decide as part of their marketing strategy to hard-code privacy protections in the design of their products, perhaps with user involvement in the development of the design, can enhance consumer trust in IoT services by reducing fears of loss of privacy.[92]

Marketing Privacy: The Case of *Apple*

As more and more information is being collected without the explicit consent of consumers, the demand for privacy protection is increasing. In an attempt to meet this demand, *Apple* increased privacy protection to restrict the government from having unfettered access to information, even for security purposes. *Apple*'s newest mobile operating system has a feature that encrypts crucial information about the users keeping it secure from thieves, the government and even themselves. Whenever a user of the new platform sets a passcode, that same code is used to lock-in their information. This new feature is a marketing pitch to a large number of people who feel an intrusion on their privacy. According to the data published by Pew Research, 86% of the people surveyed have taken steps to remove or mask their digital footprint. At the same time, 59% of Internet users do not believe it is possible to be completely anonymous online.[94] Android, *Apple*'s main competitor, is introducing this feature as well in their upcoming operating system. Note that *Apple* and Android together account for some 90% of the mobile market in the United States. One of the main devices to access the Internet, the smart phone, is already being transformed to protect consumer privacy. This is still a small step, since many apps within both operating systems are collecting other types of information such as *Facebook*, who plays a crucial role in identifying users across devices. *Apple* sought to distinguish itself by proclaiming it doesn't use customers' data to sell advertisements like *Google*.

Does government regulation to protect privacy affect innovation?[95] argue that an inherent friction exists between data-based innovation and privacy regulation. The authors examined the effect of the presence or absence of state privacy laws on the rate of adoption of Electronic Medical Record (EMR) technology and concluded that the probability of EMR adoption is lower in states with privacy laws (Fig. 3). The point is privacy regulation might restrict data dependent innovation as the IoT becomes more widespread.[96]

On the other hand, some might argue that the adverse effect on innovation occurs when access to data is restricted only to protect privacy, but this is not a fair description of what privacy regulation aims to do. Information privacy relates more to the people's ability to control and approve of what specific use is made of their information. The key issue here is using the information about individuals without their consent. Things that are mutually beneficial such as *Google*'s targeted ads might be agreeable with the masses and other activities might be viewed as intrusive, such as selling the data to a third party. The adverse impact on innovation is far less severe when firms aim to gain trust and enable the individuals to decide on their own.

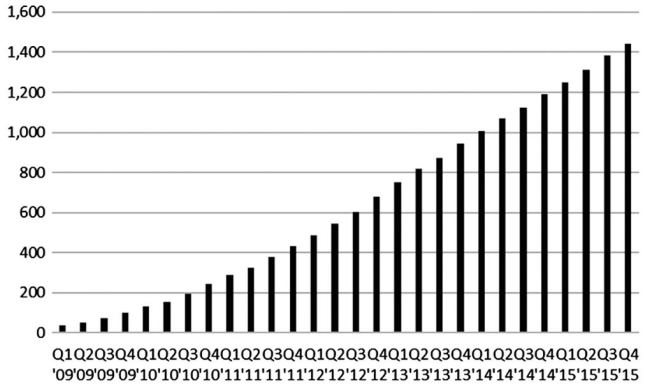

Fig. 3 — Number of mobile monthly active users worldwide 2009-2015 (in millions)[50]

Conclusion

The legal tools for protecting a competitive cyberspace marketplace are fairly robust, while the legal tools to protect consumer privacy in cyberspace is still a work in progress in the face of rapid technical change in online user tracking and Internet of Things technologies and applications. The extent of further government regulation to protect consumer privacy must be carefully balanced so as not to unduly restrict data dependent innovation because data plays vital role in various facets of society, including digital health,[97] genetic research; and FinTech.[98] The paradox of Big Data is while individuals have an ethical obligation to protect their privacy; the rapid advance of technology makes protection of privacy virtually impossible.[99] Thus while Big Data has tremendous potential; we must be cognizant of the dangers that AI and advancing data analytics will unleash upon individuals.

A new approach to data protection could be one that integrates data security and privacy by dynamically masking data until they are needed. Thus, highly granularized data can be kept safely protected by using dynamically changing pseudonymous identifiers, making it impossible to discover data values until they are revealed under controlled conditions. There are also marketing incentives for high tech firms themselves to address, with "privacy by design" innovations and other trust-building measures that can enhance their brands and reputations, the negative externalities imposed on consumers by some Internet technologies.

References

1 Rao P M & Klein J A, Strategies for high-tech firms: Marketing, economic, and legal issues, *ME Sharpe,* 2013, 138.

2 Demographic (Population) numbers in the site are based on data from the United Nations - Population Division. Internet usage information comes from data published by Nielsen Online, by ITU, the International Telecommunications Union, by GfK, by local ICT Regulators and other reliable sources, http://www.internetworldstats.com/stats.htm.

3 Smith I G (Ed.), *The Internet of Things 2012 New Horizons* (3rd ed.), 2012, http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf.

4 Pretz K, The Next Evolution of the Internet, January 2013, http://theinstitute.ieee.org/technology-focus/technology-topic/the-next-evolution-of-the-internet.

5 Blum P & Goff B, 'Internet Of Things' 101: *Legal Concerns - Law360*, 14 April 2014.

6 https://www.credit-suisse.com/ch/en/news-and-expertise/news/economy/sectors-and-companies.article.html/article/pwp/ news-and-expertise/2013/07/en/the-future-of-wearable-technology.html.

7 http://www.lawtechnologynews.com/id=1202652930046/The-Internet-of-Things-A-Legal-and-Professional-Minefield?slreturn=20140910144102.

8 Rose A, The Internet of Things has arrived — And so have massive security issues, *WIRED,* 9 January 2013, http://www.wired.com/2013/01/securing-the-internet-of-things/.

9 Think about a residential thermostat that can be adjusted *via* a smartphone and authenticated web service, or that may self-adjust based on its awareness of the homeowner's location (e.g., switching on the heating/cooling as it detects the owner nearing home), Rose A, The Internet of Things has arrived — And so have massive security issues, *WIRED,* 9 January 2013, http://www.wired.com/2013/01/securing-the-internet-of-things/.

10 Think about drug dispensers that can issue medication in response to sensing conditions in the human body through a set of apps, sensors, and other monitoring/feedback tools. Rose A, The Internet of Things has arrived — And so have massive security issues, *WIRED,* 9 January 2013, http://www.wired.com/2013/01/securing-the-internet-of-things/.

11 The *Apple* Watch is a current example of IoT, in the form of a wearable device. Wearables, like the *Apple* Watch, can track information about a person (*via* skin contact), the location (GPS), the activity, and an individuals' vital signs.

12 Fewer than 10,000 households can generate 150 million discrete points of data a day FTC, *Internet of Things Workshop*, 2013, 89.

13 For example, health or life insurance companies can use data from fitness trackers for health or life insurance rates.

14 A connected device can be used by manufactures (or hackers) to eavesdrop on the television show being watched; or the temperature at which the thermostat is set.

15 Jeffrey Rohlfs, A theory of inter-dependant demand for a communications service, *Bell Journal of Economics*, 5 (1974) 16; and Bandwagon effects in high-technology industries, *The MIT Press*, Cambridge: MA, 2003.

16 Windows is valuable because most other software is made for Windows, which increases sales of Windows; which, in turn, increases the apps that are developed for Windows.

17 *Matsushita* v *Zenith Ratio Corp*. 475 U.S. 574 (1986).

18 Sherman Act, 15 U.S. Code § 2.

19 *United States* v *Grinnell Corp*., 384 U. S. 563, 570-571 (1966). The offense of monopoly under § 2 of the Sherman Act has two elements: (1) the possession of monopoly power in the relevant market and (2) the willful acquisition or

maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident.

20 Galindo, Blanca Rodriguez 2007, Prohibition of the Abuse of a Dominant Position (The International Symposium on Anti Monopoly Enforcement); Communication from the Commission-Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings, 2009 O.J. (C 45) 7, 8.

21 http://www.cci.gov.in/sites/default/files/03201127.pdf, 39.

22 'Tying' usually refers to situations where customers that purchase one product (the tying product) are required also to purchase another product from the producer (the tied product). 'Bundling' usually refers to the way products are offered and priced by the firm. In the case of pure bundling the products are only sold jointly in fixed proportions." Galindo, Blanca Rodriguez 2007, Prohibition of the Abuse of a Dominant Position (The International Symposium on Anti Monopoly Enforcement); Communication from the Commission-Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings, 2009 O.J. (C 45) 7, 8.

23 On the other hand, however, despite this advantage *MYSpace* succumbed to competition from *Facebook*. The *Yahoo* search platforms of the 1990's were outmatched by the search algorithms of *Google* of the 2000's.

24 http://europa.eu/rapid/press-release MEMO-17-1785 en.htm.

25 *Google* is dominant in each national market for general internet search throughout the European Economic Area (EEA), that is, in all 31 EEA countries. *Google* was dominant in each country since 2008, except in the Czech Republic where the Decision found *Google* to have been dominant since 2011. Since 2008 *Google*'s search engine held very high market shares in all EEA countries, exceeding 90% in most. http://www.statista.com/statistics/267161/market-share-of-search-engines-in-the-united-states/

26 Waller S W, Antitrust and social networking, *NCL Rev*iew, 90 (2012) 1771, https://pdfs.semanticscholar.org/406e/667efbd38ff30227dbc1a5bf9f23ea12ad6a.pdf.

27 The antitrust leveraging doctrine is relevant to potential manipulation of *Google*'s dominant market power in general search to favor its own ads. Rule of Reason analysis would determine the extent of the problem in particular circumstances, but we should not underestimate customer inertia in moving from relatively easy-to-use and well branded *Google* general search to less content-rich, less well-known specialized search engines.

28 http://europa.eu/rapid/press-release_SPEECH-12-372_en.htm?locale=en.

29 http://europa.eu/rapid/press-release_IP-14-116_en.htm.

30 http://europa.eu/rapid/press-release_IP-15-4780_en.htm.

31 http://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14009_3.pdf.

32 http://europa.eu/rapid/press-release_IP-17-1784_en.htm.

33 http://www.comscore.com/Insights/Market-Rankings/comScore-Releases-April-2014-US-Search-Engine-Rankings.

34 https://www.comscore.com/Insights/Rankings/comScore-Releases-February-2016-US-Desktop-Search-Engine-Rankings

35 According to the FTC closing statement on the *Google* case. "As is well known, when a user types a word or words into a *Google* search box, *Google*, guided by proprietary algorithms, searches its index of the Internet and assembles a ranked listing of relevant websites, known as "organic" search results. These organic results – together with advertising, links to *Google* products, and other information judged to be relevant to the user's query – are returned to the user as the *Google* search results page. *Google* is a "horizontal," or general purpose, search engine because it seeks to cover the Internet as completely as possible, delivering a comprehensive list of results to any query. General purpose search engines are distinct from "vertical" search engines, which focus on narrowly defined categories of content such as shopping or travel. Although vertical search engines are not wholesale substitutes for general purpose search engines, they present consumers with an alternative to *Google* for specific categories of searches. Some vertical websites alleged that *Google* unfairly promoted its own vertical properties through changes in its search results page, such as the introduction of the "Universal Search" box, which prominently displayed *Google* vertical search results in response to certain types of queries, including shopping and local. Prominent display of *Google*'s proprietary content had the collateral effect of pushing the "ten blue links" of organic search results that *Google* had traditionally displayed farther down the search results page. Complainants also charged that *Google* manipulated its search algorithms in order to demote vertical websites that competed against *Google*'s own vertical properties." https://www.ftc.gov/system/files/documents/public_statements/295971/130103*Google*searchstmtofcomm.pdf.

36 http://www.ftc.gov/news-events/press-releases/2013/01/*Google*-agrees-change-its-business-practices-resolve-ftc.

37 Geoffrey A M & William R, *Harvard Journal of Law & Technology Occasional Paper Series* — July 2013.

38 http://cuts-international.org/pdf/Second_Preliminary_Information_report_by-CUTS.pdf.

39 http://www.cci.gov.in/sites/default/files/07302012_0.pdf.

40 http://www.cci.gov.in/sites/default/files/07302012_0.pdf, Page 3.

41 http://www.livemint.com/Companies/5D4c8f9kKB41IyL99Rfm4H/Why-did-CCI-write-*Google*-a-bad-report-card.html (The original report of the Director General could not be found on the website of the CCI).

42 The commission itself will then take its own independent view of the reports filed by the Director General. It can overrule these findings.

43 Section 4 of the *Competition Act* of 2002:
4. Abuse of dominant position.—
(1) No enterprise shall abuse its dominant position.
(2) There shall be an abuse of dominant position under sub-section (1), if an enterprise,—
(a) directly or indirectly, imposes unfair or discriminatory—
(i) condition in purchase or sale of goods or services; or
(ii) price in purchase or sale (including predatory price) of goods or service; or Explanation—For the purposes of this clause, the unfair or discriminatory condition in purchase or sale of goods or services referred to in sub-clause (i) and unfair or discriminatory price in purchase or sale of goods (including predatory price) or service referred to in sub-

clause (ii) shall not include such discriminatory conditions or prices which may be adopted to meet the competition; or
(b) limits or restricts—
(i) production of goods or provision of services or market therefor; or
(ii) technical or scientific development relating to goods or services to the prejudice of consumers; or
(c) indulges in practice or practices resulting in denial of market access; or
(d) makes conclusion of contracts subject to acceptance by other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts; or
(e) uses its dominant position in one relevant market to enter into, or protect, other relevant market.
Explanation —For the purposes of this section, the expression—
(a) "dominant position" means a position of strength, enjoyed by an enterprise, in the relevant market, in India, which enables it to—
(i) operate independently of competitive forces prevailing in the relevant market; or
(ii) affect its competitors or consumers or the relevant market in its favour;
(b) "predatory price" means the sale of goods or provision of services, at a price which is below the cost, as may be determined by regulations, of production of the goods or provision of services, with a view to reduce competition or eliminate the competitors.

44 Section 27b of the *Competition Act of India*, 2002:
"impose such penalty, as it may deem fit which shall be not more than ten percent. of the average of the turnover for the last three preceding financial years, upon each of such person or enterprises which are parties to such agreements or abuse"

45 Section 28 of the *Competition Act of India,* 2002.

46 http://www.cci.gov.in/sites/default/files/07%20%26%20%2030%20of%202012.pdf.

47 Boyd D & Ellison N, Social network sites: Definition, history and scholarship*, Journal of Computer Mediated Communication,* http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full.

48 http://techcrunch.com/2011/06/28/sean-parker-on-why-myspace-lost-to-*Facebook*/.

49 Active users are those which have logged in to *Facebook* during the last 30 days. http://www.statista.com/statistics/264810/number-of-monthly-active-*Facebook*-users-worldwide/.

50 http://www.prnewswire.com/news-releases/*Facebook*-reports-third-quarter-2013-results-229923821.html
Facebook measures "monthly active users" as users that have logged in during the past 30 days. The site defines a mobile MAU as a user who accessed *Facebook via* a mobile app or via mobile-optimized versions of the website such as m.*Facebook*.com, whether on a mobile phone or tablet such as the iPad, during the period of measurement. http://www.statista.com/statistics/277958/number-of-mobile-active-*Facebook*-users-worldwide/.

51 https://www.emarketer.com/Article/*Google-Facebook*-Increase-Their-Grip-on-Digital-Ad-Market/1015417.

52 http://files.shareholder.com/downloads/AMDA-NJ5DZ/3517992167x0x770575/481ba943-c7b2-4336-9d70-6453934517db/FB_News_2014_7_23_Financial_Releases.pdf.

53 http://www.statista.com/statistics/193538/market-share-of-net-us-digital-ad-revenues-of-*Facebook*/

54 Network effects block only frontal competition, but not lateral competition. Lateral competition means that in order to be successful, a company should not go head-to-head with the leaders in the industry, but rather find niches alongside them.

55 "If the costs of adapting are negligible, and there are no other entry barriers, the market will be perfectly competitive", Michael L Katz & Carl Shapiro, Network externalities, competition, and compatibility, *American Economic Review,* 75 (1985) 424, 426-27.

56 Grassley C, Prepared Statement by Senator Chuck Grassley of Iowa Chairman, Senate Judiciary Committee Joint hearing of the Senate Judiciary Committee and Senate Commerce Committee *Facebook*, Social Media Privacy, and the Use and Abuse of Data, 10 April 2018, https://www.judiciary.senate.gov/imo/media/doc/04-10-18%20Grassley%20Statement.pdf.

57 Jamie D, Carole C & Alice G, Watchdog to launch inquiry into misuse of data in politics, *The Guardian*, 4 March 2017, http://davelevy.info/Downloads/watchdogdatapolitics_theguardian_20170304.pdf.

58 Frank P, Beyond innovation and competition: The need for qualified transparency in internet intermediaries, *North Western University Law Review,* (2010) *104,105, 153.*

59 *Facebook*'s terms state "You will not collect users' content or information, or otherwise access *Facebook*, using auto-mated means (such as harvesting bots, robots, spiders, or scrapers) without our permission." https://www.*Facebook*.com/terms.

60 The Case of *Facebook* and *Cambridge Analytica*
a. *Cambridge Analytica* a data firm hired by the Trump 2016 Presidential Campaign gained access to private information of 50 million *Facebook* users. These included details on user identities; friend networks and user "likes". *Facebook*'s position was that what *Cambridge Analytica* did was not a "data breach", because of the consent given by its users when a *Facebook* account is opened. But *Cambridge Analytica* acknowledged that it had acquired the data through a third party violating *Facebook*'s rules prohibiting third parties of copying and transferring data.

61 Engels B, Data portability among online platforms, *Internet Policy Review*, 5 (2) (June 2016), https://policyreview.info/articles/analysis/data-portability-among-online-platforms.

62 For the EU policy on data portability "*Guidelines on the right to data portability*" 16/EN WP 242 rev.01; Adopted on 13 December 2016; last revised and adopted on 5 April 2017.

63 Pawade A S, Warad N S, Supriya R K , Swapnil S S & Sagar S H, Impact of *WhatsApp* on *Facebook, International Journal of Engineering Sciences & Research*, May 2014 http: // www.ijesrt.com.

64 Altaweel I, Good N & Hoofnagle C J, Web privacy census, *Technology Science*, (2015) 121, 502, Online.

65 Third-party tracking refers to tracking done by websites that a user never navigates to explicitly. Many Internet users are vaguely aware that their information may be collected online.

66 Libert T, Exposing the hidden web: An analysis of third-party HTTP requests on 1 million websites, *International Journal of Communication,* October, 2015, SSRN: https://ssrn.com/abstract=2685330.

67 Rao P M & Klein J A, Strategies for high-tech firms: Marketing, economic, and legal issues, *ME Sharpe,* 2013, 189.

68 Altman M, Wood A, O'Brien D R & Gasser U, Practical approaches to big data privacy over time, *International Data Privacy Law*, 12 March 2018, doi:10.1093/idpl/ipx027.

69 http://www.etsi.org/images/files/ECDirectives/2009_136.pdf.

70 Borgesius Z, Frederik, Kruikemeier, Sanne, Boerman, Sophie, Helberger & Natali, Tracking walls, take-it-or-leave-it choices, the GDPR, and the ePrivacy Regulation, *European Data Protection Law Review*, 3 (3) (2018) 353-368, SSRN: https://ssrn.com/abstract=3141290.

71 http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/beuc_en.pdf.

72 https://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/PressRelease_2014-09-30_*Google*_Administrative-Order.pdf.

73 https://www.law360.com/articles/501442?scroll=1.

74 https://www.law360.com/articles/822967/*Google*-meets-italy-s-demands-on-data-use-practices.

75 http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

76 https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf.

77 https://ec.europa.eu/info/law/law-topic/data-protection_en.

78 http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2670.

79 http://www.zdnet.com/companies-brace-for-brazil-local-data-storage-requirements-7000027092/.

80 http://www.consumerreports.org/cro/news/2014/05/most-consumers-oppose-internet-ad-tracking/index.htm.

81 Federal Trade Commission, 2012.

82 Rao P M & Klein J A, Strategies for high-tech firms: Marketing, economic, and legal issues, *ME Sharpe,* 2013, 138.

83 Evans D, The internet of things how the next evolution of the internet is changing everything, *Cisco Internet Business Solutions Group* (IBSG), April 2011.

84 https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

85 https://www.brookings.edu/blog/techtank/2018/05/23/the-general-data-protection-regulation-sets-privacy-by-default/.

86 Richards N M & Jonathan K, Three paradoxes of big data, *Stanford Law Review, Online,* 41 (2013) 66, SSRN: https://ssrn.com/abstract=2325537.

87 http://www.afcea.org/committees/cyber/documents/InternetofThingsFINAL.pdf.

88 https://www.engerati.com/article/onzo-and-kantar-use-smart-meters-evaluate-consumer-patterns.

89 https://www.law360.com/articles/526266; https://blogs.cisco.com/cle/safeguarding-privacy-in-the-internet-of-things.

90 Peppet S, Regulating the internet of things: First steps toward managing discrimination, privacy, security, and consent, *Texas Law Review*, (2014).

91 Thierer A D, The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation, *Richmond Journal of Law and Technology*, 21 (2015) 6.

92 Ward M, Connected tech sparks privacy fears, http://www.bbc.com/news/technology-25662006 (8 January 2014).

93 Federal Trade Commission, 2013, 368.

94 http://winternet.org/2013/09/05/anonymity-privacy-and-security-online/.

95 Goldfarb A & Tucker C, Privacy and innovation, *National Bureau of Economic Research,* (No. w17124) (2011).

96 Goldfarb A & Tucker C, Privacy and innovation, *National Bureau of Economic Research,* (No. w17124) (2011) Fig. 3, page 22.

97 The Affordable Care Act of 2010; digitized health care records.

98 Zetzsche Dirk A, Buckley R P, Arner D W, Barberis & Janos Nathan, From FinTech to TechFin: The regulatory challenges of data-driven finance, *New York University Journal of Law and Business,* SSRN: https://ssrn.com/abstrac=2959925 or http://dx.doi.org/10.2139/ssrn.2959925.

99 Allen Anita L, Protecting one's own privacy in a big data economy, *Harvard Law Review Forum*, 130 (2016) 71, SSRN: https://ssrn.com/abstract=2894545.