Klein, Joseph A.; Rao, P. M.

Conference Paper

Competition and consumer protection in the cyberspace marketplace

20th Biennial Conference of the International Telecommunications Society (ITS): "The Net and the Internet - Emerging Markets and Policies" , Rio de Janeiro, Brazil, 30th-03rd December, 2014

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Klein, Joseph A.; Rao, P. M. (2014) : Competition and consumer protection in the cyberspace marketplace, 20th Biennial Conference of the International Telecommunications Society (ITS): "The Net and the Internet - Emerging Markets and Policies" , Rio de Janeiro, Brazil, 30th-03rd December, 2014, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/106857

Competition and Consumer Protection in the Cyberspace Marketplace

Joseph A. Klein
Global Technology Attorney

P.M. Rao
Long Island University, Post Campus

International Telecommunications Society

20th Biennial Conference, Rio De Janeiro, November 30- December 3, 2014

Corresponding Author:
P.M. Rao
Professor and Acting Dean
College of Management
LIU Post
Brookville, New York 11548
Email: pmrao@liu.edu
Telephone: 516-299-4192

The authors thank Mohammad Azim for his excellent assistance in the research and production of this paper.

Abstract
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.

I. Growth of Internet Technology

The Internet has operated on the principle of "if you build it, people will come." The Internet's phenomenal growth is a classic example of what is known as 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 user increases.

"An industry platform with network effects leads to more users to adopt the platform, which in turn leads to more users and complementors." (Rao and Klein 2013, p. 138)
Between 2000 and 2014 the number of worldwide Internet users grew from 36 million to 2.8 billion – at an average annual rate of growth of above 17.5%.[1]

From its origins in U.S. government sponsored research, the Internet and the World Wide Web that it supports have grown exponentially in usage through a series of stages of development:

- Widespread interconnectivity of networks connecting computers worldwide according to standard protocols. Websites developed to help organize the location and retrieval of information from pages within the websites.
- The increasing ease of end user access to content made readily available from multiple sources on websites via technologically robust search engine capabilities.

[1] http://www.internetworldstats.com/stats.htm

- The rise of e-commerce ecosystems including interactive business-to-business and consumer-to-business web-accessed applications.
- The growth of social media, where individuals are not wedded to interacting with entire web pages and have more autonomy in creating, assembling, and communicating elements of personalized information virtually in real time.

A. Internet of Things

The Internet is now moving into a new significant phase of its evolution. This phase of Internet technology is referred to by Internet experts as the Internet of Things ("IoT"). (Smith 2012)
In general terms, "IoT" 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." (Pretz 2013)

"IoT" has also been described in more detail as "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." (Blum and Goff 2014)
In the "initial stages of the "IoT", identity is provided to selected objects…Value to users here comes from the interaction of these identities with other intelligent systems, such as smartphones or web services." (Rose 2013)

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, albeit limited in scope, based on that information. 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 2013)

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 smartphone 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. 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 2013)

The Apple Watch is a current example of "IoT", in the form of a wearable device. Introduced by Apple with great fanfare in September 2014, the Apple Watch "will understand who you are (authenticated via skin contact), where you are (via the iPhone's GPS), what you are doing (via gyroscope, accelerometer, and apps), and even how you are feeling (via body monitoring technologies)." (Joseph 2014)

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.[2] Gartner has predicted more generally that there will be nearly 26 billion devices on the "IoT" by 2020.[3]

In sum, the market for Internet of Things devices is here today and likely to grow very rapidly. And Internet of Things technology continues to develop 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.

II. Risks to a Competitive Marketplace and Consumer Protection

A. Competitive Market

The network effects that have helped drive the exponential growth of the Internet in the first place 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

[2] 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
[3] http://www.lawtechnologynews.com/id=1202652930046/The-Internet-of-Things-A-Legal-and-Professional-Minefield?slreturn=20140910144102

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.

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. Particularly under U.S. law dealing with the antitrust offense of monopolization,[4] 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.[5] 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.[6] However, 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 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[7], 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.

B. 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

[4] Sherman Act, 15 U.S. Code § 2.

[5] *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 571*571 or maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident."

[6] 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.

[7] Id. ("'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."

have amassed substantial market power in those markets. 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.

Consider Google, for example. Once Google achieved dominance in the search engine market – over a 90% share in the European Union[8] - 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.

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

[8] http://www.mvfglobal.com/europe

"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." (Waller 2011-2012)

An antitrust analysis of Google's alleged anti-competitive practices would proceed along similar lines used successfully in the past when applied to opening up the telecommunications market by requiring non-discriminatory access to bottleneck local exchange facilities or when applied previously to efforts to require the unbundling of such separable products as the Internet browser from Microsoft's operating software platform.[9] A search engine possessing the extent of network externalities that Google's search engine displays may be viewed as an essential facility that 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.

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:[10]

- **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

[9] http://www.justice.gov/atr/cases/f1700/1763.htm
[10] http://europa.eu/rapid/press-release_SPEECH-12-372_en.htm?locale=en

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."[11] 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."[12]

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. Unless Google improves its search practices further and lives up to its previous commitments, Google could face formal charges that may lead to large fines. (Fiveash 2014)

Europe has led the way in pursuing antitrust investigations into Google's behavior, but 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.[13]

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. The "FTC" announced a settlement in 2013 with

[11] http://europa.eu/rapid/press-release_IP-14-116_en.htm
[12] Id.
[13] http://www.comscore.com/Insights/Market-Rankings/comScore-Releases-April-2014-US-Search-Engine-Rankings

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."[14] 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."[15] 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." (Manne and Rinehart 2012)

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."[16] 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 U.S. law."[17]

Other investigations of Google's alleged abuse of its market power have been launched around the world from Latin America to Asia.

C. The Case of Facebook

Compared to the more relatively mature search engine market, currently dominated by Google, the social networking market is still developing. However, to the extent that network externalities also apply to social networks such as Facebook, the result may be the creation of entry barriers for new entrants that do not have access to the large base of users and data

[14] http://www.ftc.gov/news-events/press-releases/2013/01/google-agrees-change-its-business-practices-resolve-ftc
[15] Id.
[16] Id.
[17] Id.

regarding the users that a firmly established firm in the marketplace such as Facebook already possesses.

Facebook's social network passed 1.19 billion monthly active users as of September 2013, an increase of 18% year-over-year, dwarfing all rivals. Facebook's mobile monthly active users alone were 874 million as of September 30, 2013, an increase of 45% year-over-year.[18]

Facebook's huge number of users provides Facebook with a well-spring of user data which it can use to enable target advertising and allow favored applications developers access to the data. This gives Facebook 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." (Waller 2011-2012) 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." (Waller 2011-2012)

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

[18] http://www.prnewswire.com/news-releases/facebook-reports-third-quarter-2013-results-229923821.html

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."[19]

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," according to Waller – perhaps as high as the 60% range, depending on what firms are included in determining market share. (Waller 2011-2012) 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.[20]

As discussed earlier in this paper, 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. Waller notes 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. We are also dealing primarily with access to user information rather than to something more tangible such as hardware or software. (Waller 2011-2012)

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." (Waller 2011-2012)

In sum, 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.

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

[20] http://www.statista.com/statistics/193538/market-share-of-net-us-digital-ad-revenues-of-facebook/

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.

D. Consumer Privacy Protection

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.

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." (Rao and Klein 2013, p. 189)

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. 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.

"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." (Rao and Klein 2013, p. 189)

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.

The European Union has tried to make some headway with its Directive 2009/136/EC ("EU 2009 Directive"),[21] 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.[22] 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.

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.[23] 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.

[21] http://www.etsi.org/images/files/ECDirectives/2009_136.pdf
[22] Id.
[23] https://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/PressRelease_2014-09-30_Google_Administrative-Order.pdf

> 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."[24]

National regulators in France, Italy and Spain have challenged Google on similar grounds.[25] Other European countries are also considering challenges, but time will tell how effective they will be.

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."[26] 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.[27]

Although 85% of U.S. online consumers oppose Internet ad tracking, according to Consumer Reports,[28] 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

[24] Id.
[25] http://www.reuters.com/article/2013/06/20/google-privacy-idUSL5N0EW14X20130620
[26] http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2670
[27] http://www.zdnet.com/companies-brace-for-brazil-local-data-storage-requirements-7000027092/
[28] http://www.consumerreports.org/cro/news/2014/05/most-consumers-oppose-internet-ad-tracking/index.htm

collection and use of consumer data from Internet tracking technologies. (Federal Trade Commission 2012)

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. (Rao and Klein 2013, p. 190)

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." (Rao and Klein 2013, p. 189)

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. (Federal Trade Commission 2012)

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.

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.

"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." (Blum and Gogg 2014)

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. 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." ("FTC" Workshop 2013, p. 367) She added that "our next step will not be to propose regulations." ("FTC" Workshop 2013, p. 368)

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." (Ward 2014)

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. (Rose 2013)

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" Workshop 2013, p. 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" Workshop 2013, pp. 9-10) The development of simplified "just-in-time" notice and consumer choice options are recommended in this connection. ("FTC" Workshop 2013, p. 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. (Smith 2012, Chapter 4)

E. 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.)[29] 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? Goldfarb and Tucker (2012), 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 (Figure 1). The point is privacy regulation might restrict data dependent innovation as the "IoT" becomes more widespread.

[29] http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/

Insert Figure 1 Here

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.

III. 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. At the same time, the extent of further government regulation to protect consumer privacy must be carefully balanced so as not to unduly restrict data dependent innovation. There are 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

Blum, P., & Goff, B. (2014, April 14). 'Internet Of Things' 101: Legal Concerns - Law360. Retrieved from http://www.law360.com/articles/526266/internet-of-things-101-legal-concerns

Fiveash, K. (2014, September 23). EU dangles $6bn threat over Google in endless search abuse probe. Retrieved from http://www.theregister.co.uk/2014/09/23/almunia_warns_google_that_statement_of_objections_are_logical_next_step/

FTC. (2013). Federal Trade Commission Internet of Things Workshop ("FTC Workshop"). Washington, D.C.: Federal Trade Commission. Retrieved from http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf

FTC. (2013). *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (FTC Report, Rep.). Retrieved from http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

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

Joseph, D. (2014, September 15). Apple Watch will power the internet of things. Retrieved from http://www.theguardian.com/technology/2014/sep/15/apple-watch-internet-of-things

Leon, P., Ur, B., Shay, R., Wang, Y., Balebako, R., & Cranor, L. (2012, May). Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 589-598). ACM.

Manne, G. A., & Rinehart, W. The Market Realities that Undermined the FTC's Antitrust Case Against Google.

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

Rao, P. M., & Klein, J. A. (2013). *Strategies for High-tech Firms: Marketing, Economic, and Legal Issues*. ME Sharpe.

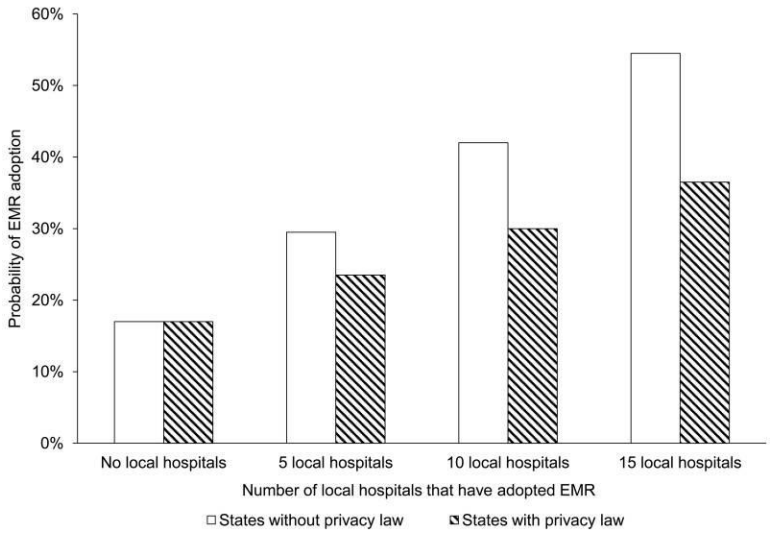
Rose, A. (2013, January 09). The Internet of Things Has Arrived — And So Have Massive Security Issues | WIRED. Retrieved from http://www.wired.com/2013/01/securing-the-internet-of-things/

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

Waller, S. W. (2011). Antitrust and Social Networking. *NCL Rev.*, *90*, 1771.

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

Figure 1. Probability of EMR Adoption in States with and without Privacy Laws



Source: Goldfarb, Avi, and Catherine Tucker. *Privacy and innovation*. No. w17124. National Bureau of Economic Research, 2011, page 81.