Before the

Federal Trade Commission

Hearings on Competition and Consumer Protection in the 21st Century
Project Number P181201

Comment on Topic 6: Evaluating the Competitive Effects of Corporate Acquisitions and Mergers

August 20, 2018

Submitted by:
Electronic Frontier Foundation
Mitchell L. Stoltz
Bennett Cyphers
815 Eddy St
San Francisco, CA 94109
(415) 436-9333
mitch@eff.org
bennett@eff.org

The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows. EFF represents over 40,000 dues-paying members, including consumers, hobbyists, artists, computer programmers, entrepreneurs, students, teachers, and researchers.

Increasing market concentration and structural barriers to competition for Internet-related businesses threaten the values of free expression, privacy, and the innovation that has made the Internet a powerful force in daily life. It is imperative that policymakers and industry address competition issues actively and thoughtfully, avoiding approaches that will themselves harm the rights and freedoms of Internet users, or impede innovation.

To protect both competition and consumers, merging of rich first-party datasets with *third-party trackers*—systems that use ads and other third-party plugins to track user habits around the web and on mobile devices—must receive

special scrutiny. Such mergers present privacy risks to users and exacerbate existing network effects and make it difficult for companies without comparable datasets to compete.

In 2007, Google purchased Doubleclick, a third-party advertising and tracking company. The merger was reviewed by the Commission at the time, and the majority determined that the competition and privacy concerns were not sufficient to challenge the acquisition. In 2013, Facebook acquired a similar product, Atlas, from Microsoft, which they have since folded into their own brands.

Today, Facebook's and Google's tracking networks are the two largest on the English-speaking Internet by far. Facebook tracking code, including social plugins and its invisible "pixel," is present on nearly 25% of the top one million sites on the Internet. The company's ad network also covers 40% of the top 500 most popular mobile apps. By some metrics, Google's reach is even broader. Rich tracking code for Doubleclick is present on over 20% of the top million sites; including Google Analytics and other services, code from Google is present on approximately three quarters of sites on the web.

In addition to their third-party tracking capabilities, both of these companies have massive first-party data stores. That gives them the ability to link data from their third party trackers with the data that users have provided them voluntarily, including real names, demographic data, contacts, communication, and interests.

We believe these kinds of mergers and acquisitions raise both privacy and competition concerns.

From a privacy perspective, mergers between tracking companies and first-party data stores create risks to users that are not present in their component parts. Normally, third-party tracking companies creates anonymous, ad-hoc profiles for users as they browse the web. They have difficulty linking one user's activity across different devices, and when a user clears cookies or switches to a new browser, the tracking company may have to start building a new profile from scratch. However, when a Facebook user browses the web, their activity can be immediately and permanently linked to their Facebook identity via Facebook's cookies. When a user uploads a photo or comments on a friend's post, they implicitly consent to giving the company their data. But when they leave facebook.com to browse the web, they may not realize that Facebook is *still tracking them*. Even if they do, the company offers no way to opt out of that

collection or to delete the data after the fact. The result is a potent, permanent profile of that user's digital life, combining data they have chosen to share with data collected surreptitiously while they might have felt anonymous.

From a competition perspective, the mergers exacerbate existing network effects and make it difficult for companies without comparable datasets to compete. They give the companies competitive advantages for both their first-party platforms and third-party advertising products. Facebook touts their ability to advertise to "real people"—that is, to use information from Facebook profiles to target individuals outside of Facebook products. Third-party ad platforms that do not possess a similar first-party dataset cannot hope to do the same. Furthermore, these companies have a privileged view of the landscape of the Internet, and therefore of their competition. This gives some companies "a relative advantage in accessing and analyzing data to discern threats well before others, including the government."[1]

There are some behavioral remedies that we believe could mitigate the harms of these mergers. After acquiring Doubleclick, Google volunteered to keep the data it collected through Doubleclick separate from the rest of its user data. Commissioner Harbour, in her dissenting statement for the investigation, predicted that the company would eventually reverse this policy, and in 2016, it did. Today, it might make sense to enforce a similar policy: require that data from third-party tracking networks must be "siloed" away from first-party data so that anonymous web activity cannot be linked to rich digital identities.

Finally, we believe traditional metrics for assessing these mergers are insufficient, and new means of evaluation are needed in the future. In her dissent, Commissioner Harbour wrote, "Traditional competition analysis of Google's acquisition of DoubleClick fails to capture the interests of all the relevant parties." We agree, and we believe that mergers between data collectors should be scrutinized more strictly than they have in the past, and on more comprehensive grounds. We hope to engage in an ongoing conversation about how to assess competitive harms caused by consolidation in the age of big data.

---

[1] *See* Maurice E. Stucke, *Should We Be Concerned About Data-opolies?*, 2 Geo. L. Tech. Rev. 275, 305 (2018) (available at https://ssrn.com/abstract=3144045 or http://dx.doi.org/10.2139/ssrn.3144045).

Before the

Federal Trade Commission

Hearings on Competition and Consumer Protection in the 21st Century
Project Number P181201

Comment on Topic 2: Competition and Consumer Protection Issues in Communication, Information, and Media Technology Networks

August 20, 2018

Submitted by:
Electronic Frontier Foundation
Mitchell L. Stoltz
Ernesto Falcon
Erica Portnoy
815 Eddy St
San Francisco, CA 94109
(415) 436-9333
mitch@eff.org
ernesto@eff.org
erica@eff.org

The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows. EFF represents over 40,000 dues-paying members, including consumers, hobbyists, artists, computer programmers, entrepreneurs, students, teachers, and researchers.

Increasing market concentration and structural barriers to competition for Internet-related businesses threaten the values of free expression, privacy, and the innovation that has made the Internet a powerful force in daily life. It is imperative that policymakers and industry address competition issues actively and thoughtfully, avoiding approaches that will themselves harm the rights and freedoms of Internet users, or impede innovation.

A. Consolidation and Centralization in Internet Platforms Threatens Freedom of Speech. Antitrust Enforcement and Other Sound Competition Policy Are Part of the Solution

The power of the Internet historically arose from its edges: innovation and growth came from its users and their contributions, rather than from a centrally controlled core of overseers. But today, for an increasing number of users, there is a powerful center to the net—and a potentially uncompetitive and unrepresentative center at that. The Internet as a whole is still vast, enabling billions of users to communicate regardless of their physical location. Billions of websites, apps, and nearly costless communications channels remain open to all. Yet too many

widely relied-upon functions are now controlled by a small number of companies. Worse, unlike previous technology cycles, the dominance of these companies has proven to be sticky. It's still easy and cheap to put up a website, build an app, or organize a group of people online—but a few large corporations dominate the key resources needed to do those things. That, in turn, gives those companies extraordinary power over speech, privacy, and innovation.

Google and Facebook dominate the tools of information discovery and the advertising networks that track users' every move across much of the Western world. Along with Apple, Microsoft, Twitter, and a few similar companies, they moderate an enormous volume of human communication. This gives them extraordinary power to censor and to surveil.

Amazon dominates online retail in the United States and back-end hosting across much of the globe, making it a chokepoint for a broad range of other services and activities. A few credit card networks process most online payments, giving them the power to starve any organization[1] that relies on sales or donations. Even more fundamentally, most people in the U.S. have little or no ability[2] to choose which company will connect them to the Internet in the first place. That gives a few broadband ISPs the power to block, throttle, and discriminate against[3] Internet users.

A lack of competition and choice impacts nearly every facet of Internet users' civil liberties. When so much of our interaction with friends, family, and broader social circles happens on Facebook, its arrangement and takedowns[4] of content matter. When so much search happens on Google, and so much video discovery on YouTube, their rankings[5] of results and recommendations matter. When Google, Facebook, and Amazon amass a huge trove of people's communications as well as data about purchases, physical movements, and Internet use, their privacy policies and practices matter. When Comcast and AT&T are the only options for fixed

---

[1] Joe Mullin, *Following Copyright Law Should Be Enough—Even When Payment Processors Say it Isn't,* EFF Deeplinks (June 8, 2018), https://www.eff.org/deeplinks/2018/06/following-copyright-law-should-be-enough-even-when-payment-processors-say-it-isnt.

[2] Ernesto Falcon, *While the Net Neutrality Fight Continues, AT&T and Verizon are Opening a New Attack on ISP Competition*, EFF Deeplinks (June 8, 2018), https://www.eff.org/deeplinks/2018/06/while-net-neutrality-fight-continues-congress-and-states-att-and-verizon-are

[3] *New Neutrality*, Electronic Frontier Foundation, https://www.eff.org/issues/net-neutrality.

[4] *Facebook, Instagram Lack Transparency on Government-Ordered Content Removal Amid Unprecedented Demands to Censor User Speech, EFF's Annual Who Has Your Back Report Shows*, Electronic Frontier Foundation (May 31, 2018), https://www.eff.org/press/releases/facebook-instagram-lack-transparency-government-ordered-content-removal-amid.

[5] Julie Samuels and Mitch Stoltz, *Google's Opaque New Policy Lets Rightsholders Dictate Search Results*, EFF Deeplinks (August 10, 2012), https://www.eff.org/deeplinks/2012/08/googles-opaque-new-policy-lets-rightsholders-dictate-search-results.

broadband Internet access for millions of people, their decisions to block, throttle or prioritize certain traffic matter.

The influence of these companies is so great that their choices can impact our lives as much as any government's. And as Amazon's recent sale of facial recognition technology to local police demonstrates, the distance between the big tech companies and government is shrinking.

Careful action to bring a variety of options back in these important portions of the Internet could re-empower users. Competition—combined with and fostered by meaningful interoperability and data portability—could let users vote with their feet by leaving a platform or service that isn't working for them and taking their data and connections to one that does. That would encourage companies to work to keep their users rather than hold them hostage.

Antitrust enforcement has played an important role in the Internet's development. The explosive growth of the Internet in the 1990s owes a lot to the Department of Justice's breakup of AT&T's telephone monopoly in the '80s. That antitrust action spurred ISPs to use the telephone system to connect people to the Internet. And the DOJ's antitrust case against Microsoft over its abuse of the Windows operating system monopoly effectively forced the company to abandon its practice of strangling new competitors in their infancy (including the nascent Google and Amazon).

A fresh look at U.S. antitrust doesn't require abandoning a rigorous approach grounded in economics and practical experience. Declines in the quality of products and services are a harm that antitrust law recognizes. And as EFF has long advocated, avoiding censorship and protecting users' privacy are at the heart of any definition of quality for a digital service or product.

B. The Commission Should Use Its Section 5 Authority to Investigate the Stalling of Fiber to the Home Deployment for High-Speed Internet Access.

The Commission requested comment on the application of its Section 5 authority to broadband Internet access markets. EFF encourages the Commission to investigate the deployment of broadband via fiber to the home (FTTH), which we believe has been artificially limited for anticompetitive reasons. In addition, absent Federal Communications Commission rules forbidding discriminatory treatment of Internet data by consumer Internet service providers (i.e., net neutrality rules), the FTC should investigate such practices to the extent of its ability. To the extent the FTC's authority over ISPs is curtailed by Supreme Court doctrines that limit the applicability of antitrust law to regulated industries, the FTC should support statutory reform.

1. Fiber to the Home Deployment Is Stagnant

Fiber to the home is a network architecture that is able to scale and upgrade at comparatively low costs while providing tremendous capacity for future Internet innovations. Yet the Federal Communication Commission's data indicate that a staggering 85 percent of Americans either cannot receive broadband services that exceed 100 Mbps, or have access to only one provider. Barely 10 percent of US consumers have access to a FTTH competitor to the local cable company delivering comparable or better speeds. Few people in the U.S. benefit from

competitors like Verizon FiOS, Google Fiber, Competitive Local Exchange Carriers, or publicly owned fiber networks.[6]

When last exploring ISP access competition and network neutrality, the FTC focused heavily on the issues of scarcity in capacity at the last mile by ISPs.[7] However, fiber optic networks have now advanced to such a degree that concerns regarding congestion are outdated.

The agency also found the market to be competitive due to competition between DSL, cable modems, satellite, and the potential entry of broadband over powerlines. With the benefit of hindsight, we now know that cable companies are effectively unchallenged in a vast majority of the US broadband market. Major telephone companies have no plans to aggressively deploy FTTH or other higher-bandwidth technologies. In fact, nearly half of American deployment in FTTH has fallen on the shoulders of small ISPs in isolated markets.[8] The complete absence of nationwide FTTH deployment plans by major ISPs should be alarming to the FTC because it has happened *after* deregulation by the FCC and billions of dollars in new corporate profits caused by the recently enacted tax cuts.[9]

The lack of competition and prospective competition in high-speed Internet access has allowed the industry to begin a trend towards monopoly status for broadband of speeds in excess of 100 mbps. Cable companies, which stand unopposed in nearly 85 percent of the market, have little need to upgrade to speeds of a gigabit or higher as their main rival, telephone companies, have opted out of doing more than upgrading their DSL lines to middle tier speeds of 25 mbps over the past few years. Wireless and satellite are not competitive alternatives at these speeds.

Online services and applications will become more dependent on high-speed connections that a majority of Americans will soon be unable to utilize or will have to utilize through their local cable monopoly. Being unable to make use of the latest advancements in Internet technologies means an impending national crisis in economic prosperity lies over the horizon as next generation application and services will not simply wait for the US market to catch up to the world. Reliance on a local cable monopoly for rapidly increasing capacity needs raises a real danger to American innovation and further exacerbates concerns regarding network neutrality.

---

[6] *See Community Network Map, supra* note 7.

[7] FEDERAL TRADE COMMISSION, *Broadband Connectivity Competition Policy*, FTC Staff Report (June 2007).

[8] Krista Tysco, *A Mid-Year Roundup of the 2017 Global FTTH Broadband Market*, PPC BROADBAND, PPC BLOG, Aug. 3, 2017, *available at* http://www.ppc-online.com/blog/a-mid-year-roundup-of-the-2017-global-ftth-broadband-market.

[9] Tax Cuts and Jobs Act of 2017, Pub. L. No. 115-97, 131 Stat. 2054; *See also* Ryan Knutson & Austen Hufford, *Verizon to Pay Down Debt, Given Employees Stock Awards with Tax Windfall*, WALL ST. J., Jan. 23, 2018, *available at* https://www.wsj.com/articles/verizon-dials-up-wireless-revenue-growth-1516714601 (reporting an extra $ 4 billion of cash on hand for Verizon); *See also* Reuters & Fortune Editors, *AT&T Is the Latest Company to Report a Tax Reform Windfall*, FORTUNE, Feb. 1, 2018, *available at* http://fortune.com/2018/02/01/att-earnings-tax-reform (reporting an extra $3 billion of cash on hand from Congress cutting corporate taxes).

2. Fiber to the Home Is the Superior Technology for Consumer Broadband.

For both copper and fiber, the basic principle of operation is the same. A cable is laid between two endpoints. The origin quickly taps out a sequence. This sequence of taps is read out at the other end. The faster the taps, the more information is received at the other end per unit time. This is referred to as a "frequency" of the data.

The frequency itself is only the first clue to understanding the total potential bandwidth, though, because a technology called "multiplexing" allows multiple frequencies to be sent over the same wire simultaneously. While there are infinite frequencies in any given range, each of which could carry its own data, the physical properties of the medium limit the number of separate "channels" that can be sent over a wire simultaneously. Frequencies that are too close will essentially blend into each other when sent over an imperfect medium.

Essentially, bandwidth depends on how quickly information can be sent along a single channel, and how many distinct channels can fit into a single cable. Therefore, the range of frequencies that a cable can support becomes vital to understanding the total bandwidth of a cable. The maximum theoretical bandwidth of a cable is a function of the range of frequencies that can be sent over that cable, along with the signal-to-noise ratio for that range.

For both the range of frequencies available and the signal-to-noise ratio, fiber greatly exceeds copper cable. For example, fiber optic cables carry information in the optical range of 400-800 THz, whereas copper transmits at the radio frequency range of up to 5000 MHz. Sending a higher frequency signal along a cable increases the amount of noise in a channel, and it does so much more punishingly for electrical signals being sent along a copper wire than for optical signals being sent along a fiber optic cable.

Copper cannot operate at higher frequencies because information degenerates more rapidly as frequency increases. Existing copper cables lose 92.8dB/km at the maximum end of their range (5000 MHz)[10]; operating at any higher frequency would only be useful at exceedingly small distances. In contrast, fiber optic cables operate at frequencies tens of thousands of times higher, and lose only 0.2 dB/km.[11] This also means that fiber optic cables are suitable for longer distance communications, thus requiring less equipment infrastructure to operate.

In practice, data does not get sent at this limit, but technological advancements in endpoint technology push us closer to that limit without replacing the existing cables. Current research focuses on how to build a device to insert data at as many frequencies as possible into the medium, to achieve bandwidths closer the theoretical limits of both copper and fiber optic cables.

---

[10] RADIO FREQUENCY SYSTEMS, *Product Datasheet*, available at http://products.rfsworld.com//WebSearchECat/datasheets/pdf/cache/LCF78-50JFNA-A0.pdf.

[11] CORNING, *Optical Fiber Product Portfolio*, available at http://www.corning.com/media/worldwide/coc/documents/Fiber/COF-006-AEN.pdf.

Previously, though the medium of optical fiber itself was significantly better for transmitting data, it was hard and expensive to build the machines to reach anywhere near that capacity. Now, technology is starting to catch up to the capacity of the medium. A 2018 study managed to put 159 Tb/s in a fiber optic cable over a thousand kilometers long.[12]

Wireless broadband faces even more challenges to be on par with FTTH. For wireless transmissions, factors such as weather, physical obstructions, distance, power levels, and competing transmissions over the same space all interfere with its ability to transmit data. The frequency that is being used for transmission also has an impact on the amount of data that can be transmitted, the distance it can travel, and its capacity to penetrate obstacles. A basic rule of thumb is the higher the frequency of the spectrum band that is being used, the more difficulty it has passing through objects. That is because the airwaves we use for wireless technologies is the same as light that would come from a flashlight (it just operates at a much lower frequency beyond visible range). In fact, we can see that from demonstration lamps being used to transmit high definition video quality data transmissions.[13]

3. Comparing the U.S. Market to International Markets Reveals How Last-Mile Internet Access Is Starved of Potential Capacity.

Today, approximately 57.8 percent of Europeans have access to DOCSIS 3.0 and FTTH with FTTH reaching 26.8 percent of EU homes and DOCSIS 3.0 reaching 44.7 percent of homes.[14] The aggregate number demonstrates how the American market is behind our European counterparts even when not every EU nation is on track to meet the metrics of universal coverage at 30 Mbps and 50 percent coverage at 100 Mbps and above by 2020.[15]

When we explore individual member states of the EU, we find that the aggregate number masks extraordinary advancements across the Atlantic that show how far behind American deployment truly is today. For example, FTTH in Portugal, Latvia, Lithuania, and Spain exceed 70 percent coverage. Spain in particular has enjoyed an extraordinary rise in FTTH coverage

---

[12] Sachiko Hirota, *Record Breaking Fiber Transmission Speed Reported*, PHYS.ORG (Apr. 16, 2018), available at https://phys.org/news/2018-04-fiber-transmission.html.

[13] Harold Hass, *Wireless data from every light bulb,* Technology, Entertainment, Design (TED) Global 2011 (Jul. 2011), http://www.ted.com/talks/harald_haas_wireless_data_from_every_light_bulb?language=en.

[14] FTTH is known as fiber-to-the-premises (FTTP) in Europe.

[15] EUROPEAN COURT OF AUDITORS, *Broadband in the EU Member States: Despite Progress, not All the Europe 2020 Targets Will be Met*, *available at* https://www.eca.europa.eu/Lists/ECADocuments/SR18_12/SR_BROADBAND_EN.pdf.

with a growth of 8.6 percent for 2017[16] as a result of a commercial co-investment and network sharing agreements.[17]

In fact, every EU member except for Ireland, Germany, the United Kingdom, Belgium, and Greece is ahead of the United States in FTTH deployment and even among those lagging nations an active rethinking or new implementation of telecom policy is occurring. For example, Ireland's fiber growth has exploded at a meteoric 419.6% increase from 2016-2017 as a result of wholesale-only initiatives.[18] The United Kingdom is currently imposing structural separation remedies on British Telecom to address their current lack of fiber deployment.[19]

Ahead of even the best-performing EU nations, South Korea has achieved near-universal deployment of fiber connections to the home.[20] Such connectivity was on display during the 2018 Winter Olympics as part of a plan by Korean ISPs to deploy the first 5G networks.[21] Such networks are reliant on fiber and were showcased during the games. Near universal coverage by fiber also allowed Korea Telecom to deploy 3D virtual reality viewing of the games[22] and support self-driving mass transit,[23] things that are simply not supportable with current U.S. infrastructure.

---

[16] EUROPEAN COMMISSION, *Broadband Coverage in Europe 2017*, *available at* https://ec.europa.eu/digital-single-market/en/news/study-broadband-coverage-europe-2017.

[17] Enrique Medina, *Why Spain is a Case Study for Super-Fast Broadband*, TELEFONICA, Nov. 20, 2017, available at https://www.telefonica.com/en/web/public-policy/blog/article/-/blogs/why-spain-is-a-case-study-for-super-fast-broadband.

[18] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Penetration and Data Usage (Growth of fibre subscriptions Dec. 2017)*, *available at* http://www.oecd.org/sti/broadband/1.11-FibreGrowth-2017-12.xls; *See also Wholesale Only Model Study supra* note 29.

[19] Ilsa Godlovitch, Bernd Sorries, & Tseveen Gantumur, *A Tale of Five Cities: The Implications of Broadband Business Models on Choice, Price and Quality*, WIK-CONSULT, Jun. 2, 2017, *available at* https://www.stokab.se/Documents/Nyheter%20bilagor/A%20tale%20of%20five%20cities.pdf.

[20] Krista Tysco, *A Mid-Year Roundup of the 2017 Global FTTH Broadband Market*, PPC BROADBAND, PPC BLOG, Aug. 3, 2017, *available at* http://www.ppc-online.com/blog/a-mid-year-roundup-of-the-2017-global-ftth-broadband-market (most noteworthy in this analysis is the role smaller ISPs play in deploying FTTH where nearly 50 percent of the growth in fiber is attributable to CLECs and local government).

[21] Erwan Lucas, *In South Korea, the Race is on for Olympics 5G Next Year*, PHYS.ORG, Feb. 28, 2017, *available at* https://phys.org/news/2017-02-south-korea-olympics-5g-year.html\.

[22] Cho Mu-Hyun, *KT to Provide 360 Degree VR for 2018 Winter Games*, ZDNET, Feb. 15, 2016, *available at* https://www.zdnet.com/article/kt-to-provide-360-degree-vr-for-2018-winter-games/.

[23] Diamond Leung, *2018 PyeongChang Olympics Has 5G-Enabled VR, Live Holograms, Self-Driving Buses, Drones*, SPORTTECHIE, Mar. 28, 2017, *available at* https://www.sporttechie.com/2018-pyeongchang-olympics-has-5g-enabled-vr-live-holograms-self-driving-buses-drones.

4. The ISP Industry Has a Persistent History of Violating Net Neutrality.

ISPs have a long history of net neutrality violations. In 2005, the FCC found that Madison River, a broadband provider based in North Carolina, had been blocking Voice over Internet Protocol (VoIP) ports, thereby preventing its customers from making use of third-party VoIP services that competed with the company's own phone services. This example of consumer harm is particularly egregious, given that "for those customers who had disconnected their traditional phone lines and were relying solely on Vonage, the blocking meant they had no ability to make calls, even to emergency 911 services."[24] The FCC's enforcement action at this time was premised on Title II of the Communications Act, to which Madison River was subject.

In 2007, Comcast was found to be interfering with legitimate traffic based solely on its type. The most widely discussed interference was with certain BitTorrent peer-to-peer (P2P) file-sharing communications, but other protocols" were also affected.[25] This interference went far beyond network management, and affected its customers' ability to download public domain works, not to mention properly use non-P2P software like Lotus Notes.

In 2012, AT&T chose to block data sent to and from users of Apple's Facetime software.[26] In particular, AT&T announced in August of 2012 that only certain, more expensive data plans would be able to use Facetime, even acknowledging that "the company was using it as a lever to get users to switch over to the new plans which charge for data usage in tiers." In other words, customers were forced to pay more to AT&T to send or receive certain types of data, based on a business decision by AT&T.

Also in 2012, Comcast announced that it would favor its own video-on-demand streaming services over third-party competitor services, by charging customers for the data they used to stream competitor services.[27] In this instance, customers were harmed by Comcast's decision to take advantage of its gatekeeper power to favor its traffic over its competitors, thereby clearly distorting the marketplace for video-on-demand services. AT&T stands ready to follow suit with its purchase of Time-Warner by engaging in discriminatory zero-rating and preferring its own content over its competitors. This type of self-dealing by AT&T is the central concern expressed in the DoJ's filings when it sued to block the merger.

---

[24] Jonathan Krim, *Phone Company Settles in Blocking of Internet Calls*, WASHINGTON POST (Mar. 4, 2005), available at http://www.washingtonpost.com/wp-dyn/content/article/2005/03/25/AR2005032501328.html.

[25] Peter Eckersley et al., *Packet Forgery By ISPs: A Report on the Comcast Affair,* ELECTRONIC FRONTIER FOUNDATION, Nov. 28, 2007, https://www.eff.org/wp/packet-forgery-isps-report-comcast-affair.

[26] David Kravets, *AT&T: Holding Facetime Hostage is No Net Neutrality Breach*, WIRED (Aug. 22, 2012), available at https://www.wired.com/2012/08/facetime-net-neutrality-flap.

[27] Kyle Orland, *Comcast: Xbox 360 On Demand Streams Won't Count Against Data Caps*, ARSTECHNICA (Mar. 26, 2012), available at https://arstechnica.com/gaming/2012/03/comcast-xbox-360-on-demand-streams-wont-count-against-data-caps.

These and many other examples[28] regularly demonstrate the gatekeeper incentive that ISPs possess and their willingness to act on that incentive.

5. FTC Authority Over Broadband ISP Practices May Be Limited.

While EFF appreciates the FTC's attention to issues of competition and discriminatory conduct in broadband Internet access markets, it is likely that the FTC cannot address these issues alone.

The FCC and FTC Memorandum of Understanding (MOU) regarding oversight of the ISP marketplace illustrates the limits of FTC authority to protect the free and open Internet.[29] It details the extent the FCC will mandate disclosure by the ISPs of their intended conduct so that the FTC can utilize its legal power to penalize deceptive assertions. At the heart of the MOU is the basic premise that so long as the industry simply tells consumers what they intend to do in the absence of federal law, self-regulation will curtail the worst practices. This is despite a majority of the public having no choice among high-speed broadband providers, a fact the FCC casually dismissed in its Order when it explicitly choose not to analyze whether high-speed broadband is a different market than low to middle tier speeds. Lastly, perhaps the main failing of this approach is that it allows ISPs to immunize from legal challenge all of the discriminatory and anticompetitive practices listed earlier so long as they disclose such practices broadly in their terms of service.

Many supporters of the Restoring Internet Freedom Order regularly assert that antitrust law can substitute for many of the concerns raised by consumer groups. This presumes enforcement by the FTC and Department of Justice. In practice, Supreme Court doctrine weighs heavily in favor of expert regulators having primary jurisdiction. In fact, the FTC itself told Congress in 2010 that if the current status of antitrust law had been in place 40 years ago, the Department of Justice prosecution of AT&T's monopoly would have likely failed.[30]

Nowhere within the Restoring Internet Freedom Order does the FCC even attempt to address the impact of the two seminal Supreme Court cases known as *Trinko*[31] and *Credit*

---

[28] Tim Karr, *Network Neutrality Violations: A Brief History*, Free Press (Apr. 25, 2017), available at https://www.freepress.net/blog/2017/04/25/net-neutrality-violations-brief-history.

[29] FEDERAL COMMUNICATIONS COMMISSION AND FEDERAL TRADE COMMISSION CONSUMER PROTECTION MEMORANDUM OF UNDERSTANDING, available at https://www.ftc.gov/system/files/documents/cooperation_agreements/151116ftcfcc-mou.pdf.

[30] Prepared Statement of the Federal Trade Commission, Committee on Judiciary: *Is There Life After Trinko and Credit Suiise? The Role of Antitrust in Regulated Industries* (June 15, 2010), available at https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-courts-and-competition-policy-committee-judiciary-united/100615antitrusttestimony.pdf.

[31] *Verizon Communications, Inc*. v. *Law Offices of Curtis V. Trinko*, 540 U.S. 398 (2004).

Suisse[32] despite invoking antitrust law enforcement more than 150 times as a fallback enforcement power. Rather, consumers are presented an overly optimistic prognosis of how antitrust law will remedy many of the pending market failures to justify total abdication of responsibility over a critical service for all Americans. To the extent that collusive conduct that would run afoul of antitrust laws take place within the ISP market, the FCC's abandonment of its role as regulator has the potential to create a major obstacle to antitrust enforcement.

Accordingly, while the FTC should vigorously enforce Section 5 with respect to broadband ISPs, it should also recommend affirmative rules on discriminatory conduct by ISPs.

[32] *Credit Suisse Securities* v. *Billing*, 551 U.S. 264 (2007).

Before the

Federal Trade Commission

Hearings on Competition and Consumer Protection in the 21st Century
Project Number P181201

Comments on Topic 3: The Identification and Measurement of Market Power and Entry Barriers, and the Evaluation of Collusive, Exclusionary, or Predatory Conduct or Conduct that Violates the Consumer Protection Statutes Enforced by the FTC, in Markets Featuring "Platform" Businesses

August 20, 2018

Submitted by:
Electronic Frontier Foundation
Bennett Cyphers
Jamie L. Williams
815 Eddy St
San Francisco, CA 94109
(415) 436-9333
bennett@eff.org
jamie@eff.org

The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows. EFF represents over 40,000 dues-paying members, including consumers, hobbyists, artists, computer programmers, entrepreneurs, students, teachers, and researchers.

Increasing market concentration and structural barriers to competition for Internet-related businesses threaten the values of free expression, privacy, and the innovation that has made the Internet a powerful force in daily life. It is imperative that policymakers and industry address competition issues actively and thoughtfully, avoiding approaches that will themselves harm the rights and freedoms of Internet users, or impede innovation.

A. Lack of Access to Data—and Lack of User Control Over Data—Is an Entry Barrier in Markets Featuring Platform Businesses.

In today's data-driven world, access to data is critical for competition—particularly in markets featuring platform businesses and social networks. The web's largest platforms are well aware of this; their companies were built on consumer data. These same companies are now attempting to stop competition by cutting off competitors' access to publicly available data, blocking interoperable technologies, and failing to give users any meaningful ability to transport their data to other platforms. This is a threat to competition.

Facebook and its subsidiaries, for example, are over ten times more valuable than the next two largest social media companies outside China—Twitter and Snapchat—combined. The social media giant has cemented its dominance by buying out potential competitors before they've had a chance to grow (like Instagram) and waging wars of attrition against others (like Snapchat) when it can't. Because of its massive reach across much of the world, the platform can effectively censor public speech,[1] perform psychological experiments,[2] and potentially sway elections on the scale of a nation-state. If users don't like the way Facebook wields this power, there is nowhere else as ubiquitous or as well populated for them to go. Facebook's trove of user data is its most valuable asset, which presents a dilemma. Thanks to ***network effects***,[3] every user who joins a social network makes it more valuable for advertisers and more useful to everyone else. Without some access to the data Facebook has, it is virtually impossible for upstart platforms to compete with the behemoth now used by nearly a third of the world.[4]

To protect consumers and ensure competition in a data-driven world, two things are needed.

First, Internet users must be given meaningful control of their own data. They must have an affirmative right to data access and "data portability," so they can get a complete copy of their data from a service provider and move it to a different platform. The data should be easy to understand, machine-readable, and available in widely adopted standard formats when applicable.

Second, the Commission must take into account efforts by large platforms to maintain monopolistic control over Internet users and their data in its analysis of competition and consumer protection issues. Such behavior is predatory and exclusionary, and a threat not only to competition, but also to consumers' online civil liberties. Consumers suffer when they have to rely on just a few platforms to communicate and learn online, and to protect their rights. Those few, dominant platforms have little incentive to protect user privacy, and sometimes even to maintain robust security practices to protect users, and they often substitute their own view of what constitutes valuable speech for that of their users or the broader public.

B. Major Internet Platforms Are Using Computer Crime Statutes to Maintain Monopolistic Control Over Data and to Conduct Exclusionary and Predatory Behavior Under Color of the Law.

One area of exclusionary and predatory conduct the Commission should pay careful attention to is large platforms abusing existing laws to maintain monopolistic control over user data. Specifically, major Internet companies are currently attempting to co-opt a notoriously

---

[1] https://www.onlinecensorship.org/.

[2] https://www.theguardian.com/technology/2014/jul/02/facebook-apologises-psychological-experiments-on-users.

[3] https://www.vox.com/videos/2018/4/11/17226430/facebook-network-effect-video-explainer.

[4] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

imprecise, pre-Internet criminal anti-"hacking" statute intended to target computer break-ins, the Computer Fraud and Abuse Act ("CFAA"), and their state law equivalents, and transform these laws into tools for conducting anti-competitive behavior under the color of the law.[5] To protect comptition, abuse of the CFAA must stop.

Congress passed the CFAA—which has been dubbed the "worst law in technology"[6]—in 1986, in response to a series of malicious computer break-ins. The law makes it a crime to access a computer "without authorization" but fails to tell us what that means. This vague language has enabled the law to metastasize in some jurisdictions from a law meant to target malicious "hacking" of private computer systems, into a tool for companies and websites to selectively enforce their computer use preferences and policies—such as terms of service prohibitions on using automated web browsing tools to access information—against competitors.

Platforms have taken advantage of this in a number of ways. In recent years, large companies—including Microsoft-owned LinkedIn[7]—have amped up efforts to use the CFAA's civil enforcement provision to punish competitors for using commonplace automated web browsing tools to access information they've published publicly online for the rest of the world to see. As USC Gould Law Professor Orin Kerr has explained, however, posting information publicly on the web and then telling someone they are not authorized to access it is "like publishing a newspaper but then forbidding someone to read it."[8] This is a clear abuse of a law meant to target criminals.

Automated web browsing—also referred to as "web scraping"[9]—is the process of using a computer script to send tailored queries to websites to retrieve specific pieces of content. The technique is used across the web for countless applications, such as aggregating information from multiple sources and identifying and extracting data for analysis.

The web is the largest, ever-growing data source on the planet. It's a critical resource for journalists, academics, businesses, and everyday people alike. Meaningful access sometimes requires the assistance of technology, to automate and expedite an otherwise tedious process of accessing, collecting and analyzing public information. As a technical matter, web scraping is simply machine automated web browsing. There is nothing that can be done with a web scraper that cannot be done by a human with a web browser. As one district court judge recently recognized, web scraping "is merely a technological advance that makes information collection easier; it is not meaningfully different from using a tape recorder instead of taking written notes,

---

[5] *See generally* Jamie L. Williams, *Automation is Not "Hacking": Why Courts Must Reject Attempts to Use the CFAA as an Anti-Competitive Sword*, 24 B.U. J. Sci. & Tech. L. X (forthcoming 2018) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3234076).

[6] https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology.

[7] https://www.eff.org/deeplinks/2017/08/judge-cracks-down-linkedins-shameful-abuse-computer-break-law.

[8] *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1169 (2016).

[9] https://www.eff.org/deeplinks/2018/04/scraping-just-automated-access-and-everyone-does-it.

or using the panorama function on a smartphone instead of taking a series of photos from different positions."[10]

Use of automated web browsing can help competition by lowering startup information barriers[11] and enable consumers to find deals and discounts online.[12] It can also help uncover unfair deceptive business practices. ProPublica, for example, used automated web browsing to uncover that Amazon's pricing algorithm was hiding the best deals from its customers.[13] And because broader access to datasets can help correct bias in how algorithms are currently trained, it can also help identify and correct issues of algorithmic bias.[14]

It is important to understand that web scraping is a *widely used* method of interacting with the content on the web: everyone does it—even (and especially) the companies trying to convince courts to punish others for the same behavior. Companies use automated web browsing products to gather web data for a wide variety of uses.[15] Some examples from industry include manufacturers tracking the performance ranking of products in the search results of retailer websites, companies monitoring information posted publicly on social media to keep tabs on issues that require customer support, and businesses staying up to date on news stories relevant to their industry across multiple sources. E-commerce businesses use automated web browsing to monitor competitors' pricing and inventory, and to aggregate information to help manage supply chains. Businesses also use automated web browsers to monitor websites for fraud, perform due diligence checks on their customers and suppliers, and to collect market data to help plan for the future. Gartner has even recommended that all businesses treat the web as their largest data source and predicts that the ability to compete in the digital economy will depend on the ability to curate and leverage web data: "Your company's biggest database isn't your . . . internal database. Rather it's the Web itself."[16]

---

[10] *Sandvig v. Sessions*, No. CV 16-1368 (JDB), 2018 WL 1568881, at *7 (D.D.C. Mar. 30, 2018).

[11] *See* Rory Van Loo, *Rise of the Digital Regulator*, 66 Duke L.J. 1267, 1285–89 (2017).

[12] *See* Complaint, *Sw. Airlines Co. v. Roundpipe LLC*, No. 3:18-CV-33 (N.D. Tex. filed Jan. 5, 2018) (lawsuit by Southwest Airlines against a company that used automated web browsing software to enable customers to check flight prices and take advantage of the airline's own rebooking deals).

[13] https://www.propublica.org/article/how-we-analyzed-amazons-shopping-algorithm.

[14] *See* Amanda Levendowski, *How Copyright Law Can Fix AI' s Implicit Bias Problem*, 93 Wash. L. Rev. (forthcoming 2018).

[15] https://www.import.io/post/13-ways-use-web-scraping-tools/.

[16] https://www.forbes.com/sites/gartnergroup/2015/02/12/gartner-predicts-three-big-data-trends-for-business-intelligence/.

Even the very companies trying to misuse the CFAA to punish competitors for using automated web browsing tools have used—and continue to use—these same techniques to build their businesses.[17]

Boston University Law Professor Andrew Sellars recently analyzed the sixty-one opinions generated via web scraping cases in the last twenty years. He reported that the "vast majority of these opinions concern claims brought by direct commercial competitors or companies in closely adjacent markets to each other."[18] The CFAA is first and foremost a criminal statute. The fact that these unauthorized Web scraping cases are *consistently* about blocking competition—and not about punishing criminals who break into private computer systems—demonstrates that the law is clearly being abused.

The companies seeking to abuse the CFAA in this way are subverting the web's open access norms.[19] These short-sighted and opportunistic efforts threaten open access to information across the Internet, including by investigative journalists, researchers, academics, and individual consumers. And in an era of algorithms and artificial intelligence, lack of access to data is a barrier to product innovation.

LinkedIn characterizes its reliance on the CFAA as about protecting user privacy, not about stifling competition.[20] But the company's proposed rule—imposing criminal CFAA liability for automated access of publicly available user data by competitors that LinkedIn has told to "go away"—will not truly protect the privacy interests of LinkedIn users who decide to publish their information publicly online. The data will still be freely available on the web for anyone else to access and use, without consequence. LinkedIn's privacy policy acknowledges the inherent lack of privacy in data users post publicly on its site and makes no promises to users about LinkedIn's ability to protect it: "Please do not post or add personal data to your profile that you would not want to be publicly available."[21] What is needed to protect privacy is

---

[17] Microsoft-owned LinkedIn, for example, one company seeking to use the CFAA to block automated Web scraping by a competing service, acknowledges in its privacy policy that it uses automated tools, *i.e.*, Web scraping, to "collect public information about you, such as professional-related news and accomplishments" and makes that information available on its own website—unless a user opts out via adjusting their default privacy settings. *See* LinkedIn, Privacy Policy, §§ 1.1-1.2 (effective May 8, 2018), https://www.linkedin.com/legal/privacy-policy.

[18] *See* Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. Sci. & Tech. L. 424, X (forthcoming 2018) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3221625).

[19] *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1162–64 (2016) (available at https://columbialawreview.org/content/norms-of-computer-trespass/).

[20] See *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1106 (N.D. Cal. 2017).

[21] See LinkedIn, Privacy Policy, § 1.1 (effective May 8, 2018), https://www.linkedin.com/legal/privacy-policy.

comprehensive, thoughtful privacy regulation that LinkedIn, its parent company Microsoft, and all other websites and Internet service providers would be subject to.[22]

Platforms have also used the CFAA to go after companies for creating interoperable software and to shut down follow-on innovation. Social media giant Facebook, for example, for a decade has pursued litigation against a company that tried back in 2008 to provide a social media aggregation service for users of Facebook and other social media platforms.[23] This service, had it not been stifled in the cradle, could have been a great boon to those who often switch between services like Facebook, LinkedIn, and Twitter, or who struggle to remember who's a friend, who's a contact, and who's a follower, or where they received any given message. Facebook sent the company, Power Ventures, a cease and desist letter and set up an ineffective IP address block. When Power continued to provide its social media aggregation services to Facebook users, Facebook turned to the CFAA. In order to provide its aggregation services, Power Ventures had used—with permission—the valid Facebook login credentials of its users. Facebook claimed that Power Ventures had violated the CFAA by continuing to use these valid credentials after receipt of the cease and desist letter. And in 2016, it convinced the Ninth Circuit to go along with this theory of liability. At Facebook's urging, the court contorted previously clear CFAA precedent and opened the door for even more abuse of the CFAA,[24] including many of the pending automated web browsing cases that are threatening competition and open access across the web today (which consistently rely on this Ninth Circuit decision).

C. Because Data Is a Measure of Market Power, Mergers Involving Data from Third-Party Trackers—Including User Location Data—Must Receive Special Scrutiny.

Finally, to protect both competition and consumers, merging of rich first-party datasets with *third-party trackers*—systems that use ads and other third-party plugins to track user habits around the web and on mobile devices—must receive special scrutiny. Such mergers present privacy risks to users and exacerbate existing network effects, and they make it difficult for companies without comparable datasets to compete.

In 2007, Google purchased Doubleclick, a third-party advertising and tracking company. The merger was reviewed by the Commission at the time, and the majority determined that the competition and privacy concerns were not sufficient to challenge the acquisition. In 2013, Facebook acquired a similar product, Atlas, from Microsoft, which they have since folded into their own brands.

Today, Facebook and Google's tracking networks are the two largest on the English-speaking Internet by far. Facebook tracking code, including social plugins and its invisible

---

[22] *See, e.g.*, https://www.eff.org/deeplinks/2018/08/how-improve-california-consumer-privacy-act-2018; *see also* EFF Comments submitted in response to Topic #4 (FTC_P181201), Sec. B.

[23] https://www.eff.org/cases/facebook-v-power-ventures.

[24] https://www.eff.org/deeplinks/2016/12/take-two-ninth-circuit-revises-two-password-sharing-decisions-fails-fix-cfaa-mess.

"pixel," is present on nearly 25% of the top one million sites on the Internet. The company's ad network also covers 40% of the top 500 most popular mobile apps. By some metrics, Google's reach is even broader. Rich tracking code for Doubleclick is present on over 20% of the top million sites; including Google Analytics and other services, code from Google is present on approximately three quarters of sites on the web.

In addition to their third-party tracking capabilities, both of these companies have massive first-party data stores. That gives them the ability to link data from their third party trackers with the data that users have provided them voluntarily, including real names, demographic data, contacts, communication, and interests.

We believe these kinds of mergers and acquisitions raise both privacy and competition concerns.

From a privacy perspective, mergers between tracking companies and first-party data stores create risks to users that are not present in their component parts. Normally, third-party tracking companies creates anonymous, ad-hoc profiles for users as they browse the web. They have difficulty linking one user's activity across different devices, and when a user clears cookies or switches to a new browser, the tracking company may have to start building a new profile from scratch. However, when a Facebook user browses the web, their activity can be immediately and permanently linked to their Facebook identity via Facebook's cookies. When a user uploads a photo or comments on a friend's post, they implicitly consent to giving the company their data. But when they leave facebook.com to browse the web, they may not realize that Facebook is *still tracking them*. Even if they do, the company offers no way to opt out of that collection or to delete the data after the fact. The result is a potent, permanent profile of that user's digital life, combining data they have chosen to share with data collected surreptitiously while they might have felt anonymous.

From a competition perspective, *these mergers exacerbate existing network effects* and make it difficult for companies without comparable datasets to compete. They give the companies competitive advantages for both their first-party platforms and third-party advertising products. Facebook touts their ability to advertise to "real people"—that is, to use information from Facebook profiles to target individuals outside of Facebook products. Third-party ad platforms that do not possess a similar first-party dataset cannot hope to do the same. Furthermore, these companies have a privileged view of the landscape of the Internet, and therefore of their competition. This gives some companies "a relative advantage in accessing and analyzing data to discern threats well before others, including the government."[25]

There are some behavioral remedies that we believe could mitigate the harms of these mergers. After acquiring Doubleclick, Google volunteered to keep the data it collected through Doubleclick separate from the rest of its user data. Commissioner Harbour, in her dissenting statement for the investigation, predicted that the company would eventually reverse this policy,

[25] *See* Maurice E. Stucke, *Should We Be Concerned About Data-opolies?*, 2 Geo. L. Tech. Rev. 275, 305 (2018) (available at https://ssrn.com/abstract=3144045 or http://dx.doi.org/10.2139/ssrn.3144045).

and in 2016, it did. Today, it might make sense to enforce a similar policy: require that data from third-party tracking networks must be "siloed" away from first-party data so that anonymous web activity cannot be linked to rich digital identities.

Finally, we believe traditional metrics for assessing these mergers are insufficient, and new means of evaluation are needed in the future. In her dissent, Commissioner Harbour wrote, "Traditional competition analysis of Google's acquisition of DoubleClick fails to capture the interests of all the relevant parties." We agree, and we believe that mergers between data collectors should be scrutinized more strictly than they have in the past, and on more comprehensive grounds. We hope to engage in an ongoing conversation about how to assess competitive harms caused by consolidation in the age of big data.

Before the

Federal Trade Commission

Hearings on Competition and Consumer Protection in the 21st Century
Project Number P181201

Comments on Topic 8: The Role of Intellectual Property and Competition Policy in Promoting Innovation

August 17, 2018

Submitted by:
Electronic Frontier Foundation
Corynne McSherry
Alex Moss
815 Eddy St
San Francisco, CA 94109
(415) 436-9333
corynne@eff.org
alex@eff.org

The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows. EFF represents over 40,000 dues-paying members, including consumers, hobbyists, artists, computer programmers, entrepreneurs, students, teachers, and researchers.

Increasing market concentration and structural barriers to competition for Internet-related businesses threaten the values of free expression, privacy, and the innovation that has made the Internet a powerful force in daily life. It is imperative that policymakers and industry address competition issues actively and thoughtfully, avoiding approaches that will themselves harm the rights and freedoms of Internet users, or impede innovation.

Thoughtful, balanced approaches to patent and copyright policy are vital to advancing all of the societal values that digital technology should embody. The FTC has an important role to play in ensuring that intellectual property rights are enforced and licensed in ways that promote innovation, including by creating incentives and opportunities for access to emerging markets and technologies. Too often, the core principles of intellectual property and antitrust are depicted as inherently in tension. In fact, both areas of law serve the same goal of promoting innovation and thus economic growth and consumer welfare. The FTC's vigilant enforcement of antitrust laws, including against abuses of intellectual property rights, is crucial to ensuring those goals are served. Otherwise, the power to exclude—the power that patents and copyrights confer—will be misused in ways that imperil what they exist to ensure: the future of innovation in this country.

These comments address several ways in which intellectual property laws and related uses of contract law act to inhibit competition and innovation: the assertion of patents that cover essential aspects of standards, the abuse of licensing terms attached to copyrighted software and other digital products, Section 1201 of the Digital Millennium Copyright Act, and expansive applications of copyright law to software.

A. Antitrust Enforcement Regarding Standards-Essential Patents

EFF wishes to emphasize the potential for harmful business conduct, and thus the need for vigilant and active FTC enforcement of antitrust laws, in connection with intellectual property rights covering technology essential to industry standards. Standards are industry conventions that allow for compatibility and interoperability between different suppliers' products and services. For example, the protocols that allow users to communicate over the Internet are standards. Because of the interoperability these standards allow, more people can communicate with each other than at any time in history.

Because standards facilitate interoperability, they enhance competition, innovation, and consumer choice. Companies don't need to compete over their ability to implement a standard because the same information is available to all who wish to implement the standard, allowing them all to achieve the same level of technical efficiency through implementation. This removes barriers to entry for new implementers, thus ensuring that consumers' preferences on other features drives market behavior, which in turn promotes new developments and further innovation.

At the same time, the power that comes from standardization creates the possibility for abuse when combined with the power to exclude that comes from patents. Standards-essential patents (or "SEPs") are patents that cover technically or commercially necessary ("essential") aspects of an industry standard. SEP owners are thus able to charge anyone who makes, sells, or uses a standards-compliant device with infringement on the ground that these activities practice the standard and thus necessarily infringe the SEPs relevant to that standard. Small businesses are particularly vulnerable to these charges because of the exorbitant costs of mounting a successful litigation defense, especially when the infringement charges implicate a huge number of patents because so many are considered "essential" to the standard.

EFF urges the FTC to undertake active and vigilant enforcement efforts to prevent and minimize the harm from of abusive business practices involving standards-essential patents.

1. Standard Setting and RAND Obligations

Standard setting is crucial for innovation in the networked world. The Internet, as a network of networks operated by many thousands of entities, could not exist without standards. There is, nonetheless, the potential for harm to occur as a result of the standard-setting process because it requires a high degree of cooperation and collaboration between industry participants who generally compete with each other in downstream markets.

Standard-setting organizations ("SSOs") have the ability to mitigate these harms by imposing requirements on those participating in the standard-setting process. Importantly, SSOs generally require participants to commit to licensing any SEPs on terms that are fair, reasonable

and non-discriminatory ("FRAND" or "RAND" obligations). Because RAND obligations commit SEP owners to making their patents available to licensees, they prevent them from using the right to exclude that they would otherwise have. RAND obligations ensure market access to third parties, including competitors of those directly involved in standard-setting processes.

EFF urges the FTC to recognize the benefits of standard-setting processes to innovation, but also to ensure obligations are imposed on licensors that require the standardized technologies to be accessible to all implementers at fair, reasonable, and non-discriminatory rates vis a vis similarly-situated licensees.

2. SEP Pooling Arrangements

Industry standards are often highly complex and multifaceted, incorporating many distinct technologies that implicate hundreds or thousands of individual patents. For both licensor and licensee, the time and money it would take to negotiate individual licenses is prohibitive. SEPs are thus often licensed together with one entity or administrator licensing many different rightsholders' SEPs. Bundled licenses for SEPs are pro-innovation to the extent that these licenses reduce transaction costs while providing certainty and freedom to operate.

These bundles also create the potential for substantial harm because of the power that SEP owners have once the relevant standard has been adopted. Consumers and suppliers can find themselves effectively "locked in" to a particular standard, and thus to the SEPs it implicates.

Pool licenses may harm innovation and competition alike if they include SEPs relevant to different standards that compete against each other for adoption. In that case, having the same entity or entities license both sets of SEPs could harm innovation by favoring one standard over the other for reasons that have nothing to do with technology, functionality, or consumer choice. While SEP pool licenses should be considered potentially beneficial, the FTC should ensure that pool licenses are limited to SEPs relevant to a particular standard or to standards that complete rather than compete against each other.

As a corollary, pool licenses also give rightsholders the ability to distort downstream product markets, where they may compete with other implementers who were not involved in the standard-setting process, and who possess no SEPs. Implementers must not be disadvantaged by their direct competitors through control of SEPs. Pool licensing activities that have the intent or effect of disadvantaging rivals of pool licensors (or their privies) should be viewed as anticompetitive and harmful to innovation.

EFF urges the FTC to recognize the benefits of pool SEP licenses as well as the potential for harm from the pooling of SEPs relevant to competing standards or extraction of unfair advantages in downstream product markets.

3. SEP Licensing and Licensee Obligations

Whether or not SEPs are licensed together as a package, SEP licenses can include terms that distort markets and corrode the benefits that flow from standardization. As discussed above, RAND obligations are crucial to ensuring that standards which implicate SEPs are accessible to

similarly situated implementers regardless of involvement in SSOs. Unfortunately, it is difficult, if not impossible, to determine *ex ante* during the process of standard-setting what reasonable and non-discriminatory rates will be once the standard is actually put to use and adopted by the market. As such, licensors and licensees are often left to negotiate for themselves what the obligation will actually require, and to do so after the lock-in effects of standardization have set in.

Recently, courts have begun to give teeth to RAND obligations in judicial decisions assessing licensors' fidelity with their RAND obligations and determining in numerical terms what RAND rates should be.[1] However, undertaking such defensive litigation is extremely expensive, time-consuming, and uncertain. As a result, companies without deep pockets may face practical constraints that limit their ability to challenge offers for SEP licenses as violating the licensor's RAND obligations.

One of the most effective ways to ensure that SEP licenses qualify as RAND is by disclosing the terms of those licenses, at least with respect to non-proprietary information such as the duration of the license and royalty rate or lump sum which the licensee has paid. Transparency for those license terms will help give implementers the information necessary to determine if the offer provided to them is actually reasonable and non-discriminatory in comparison to the license terms of similarly-situated implementers of the standard.

The FTC should also ensure that SEP licensors, whether acting alone or in concert, make clear to licensees which patents are included in a license and which aspects of the standard those patents cover. That way, licensees can assess meaningfully whether an SEP license offer is reasonable and non-discriminatory based on the value of the patented technology rather than the standard into which suppliers and consumers have already been locked in. This approach also promotes innovation by ensuring developers have the information they need to, if possible, design around existing patents to make new technological advances.

Despite the importance of transparency, many SEP licensors choose to keep their license terms secret, and conceal any disputes that arise over their rights by requiring binding arbitration. As a result, the public has far too little knowledge as to the actual terms of SEP licenses. EFF is particularly concerned that these licenses include terms that are harmful to innovation and abusive of the powers the federal patent grant confers. For example, licenses may impose draconian penalties on licensees who challenge the substantive patentability of the SEPs included in the license—or provide assistance to challenges that others raise. The FTC should view such terms as antithetical to innovation, competition, and the First Amendment's guarantee of access to the courts. Patent owners must not be able to use their power to exclude people from using of an industry standard to silence those who wish to challenge the substantive merits of SEPs relevant

[1] *See, e.g., TCL Commc'n Tech. Holdings, Ltd. v. Telefonaktiebolaget LM Ericsson*, No. CV 15-2370 JVS(DFMX), 2017 WL 6611635, at *49 (C.D. Cal. Dec. 21, 2017); *In re Innovatio IP Ventures, LLC Patent Litig.*, No. 11 C 9308, 2013 WL 5593609, at *2 (N.D. Ill. Oct. 3, 2013); *Microsoft Corp. v. Motorola, Inc.*, No. C10-1823JLR, 2013 WL 2111217, at *37 (W.D. Wash. Apr. 25, 2013).

to that standard. When weak patents are permitted to stand, the result is a tax on the kind of innovation and productivity that is necessary for continued technological and economic growth.

B. Abuse of License Agreements and Terms of Service on Digital Goods

While the Commission is rightly concerned with the effect of patents on competition, given the nature of online expression and commerce, the Commission should be equally if not more concerned with another IP doctrine: copyright. Copyrighted content, including software, is generally licensed, and those licenses can come with onerous terms. Traditionally, once a person has purchased a product, she is free to use it however she sees fit without oversight or control from the copyright owner. Purchasers have also been free to use competitors' add-on software and hardware that interoperate with the goods they buy, because innovators have been able to develop and distribute such technologies.

That expectation is upended when it comes to products that come with embedded software, from tractors[2] to refrigerators to toasters[3] and children's toys.[4] That software is supposed to make our stuff smarter, but it also makes our stuff not really ours. We own the hardware, but we only *license* the software in it. And those licensing agreements not only limit consumers ability to repair, test, and reuse consumer products, they also inhibit add-on innovation.

Those limits generally take two forms. First, they force customers to waive statutory rights like fair use, the right to reverse engineer (to understand non-copyrightable elements or to create interoperable software and hardware); to perform security or other research[5] involving the software; or to perform otherwise lawful acts of circumvention,[6] such as device jailbreaking. Second, they impose conditions on use of the product, including forbidding use of "unauthorized" hardware or software[7] in conjunction with the device (such as third-party replacement parts for repair, competing peripherals, or privacy-protecting software on mobile phones).

---

[2] *See* Kit Walsh, "John Deere Really Doesn't Want You to Own That Tractor", EFF Deeplinks (December 20, 2016), https://www.eff.org/deeplinks/2016/12/john-deere-really-doesnt-want-you-own-tractor.

[3] *See* Violet Blue, "That time your toaster broke the internet", Engadget, (October 28, 2016) https://www.engadget.com/2016/10/28/that-time-your-smart-toaster-broke-the-internet/.

[4] *See* Cory Doctorow, "The latest generation of chatbot toys listen to your kids 24/7 and send their speech to a military contractor", boingboing (December 7, 2016), https://boingboing.net/2016/12/07/the-latest-generation-of-chatb.html.

[5] *See* Cory Doctorow, "Oracle's CSO demands an end to customers checking Oracle products for defects", boingboing (August 11, 2015), https://boingboing.net/2015/08/11/oracles-cso-demands-an-end-t.html.

[6] *See* PLAYSTATION®4 SYSTEM SOFTWARE LICENSE AGREEMENT (Version 2.0), https://doc.dl.playstation.net/doc/ps4-eula/ps4_eula_en.html.

[7] *See* "Microsoft's EULA Allows Them to Disable Pirated Games", GameRant, https://gamerant.com/microsoft-pirate-game-disable-110/.

Users who violate these terms can find themselves threatened with a copyright lawsuit, but that is relatively rare. A more common tactic is to threaten third parties who want to offer add-on products or services (including repair) that might conflict with the EULA terms.

C. Section 1201 of the Digital Millennium Copyright Act

Section 1201 of the Digital Millennium Copyright Act was ostensibly intended to stop copyright infringers from defeating anti-piracy protections added to copyrighted works. In practice, however, the anti-circumvention provisions have been used to stifle a wide array of legitimate activities.

Traditionally, once a consumer has purchased a product, she has been free to use it however she sees fit. Legitimate consumers of electronic goods have been free to customize their products to better fit their needs; just as car enthusiasts might wish to soup up their engines, consumers may wish to write their own software for their robot pet, install a larger hard drive on their computer, etc. Consumers have also traditionally been free to choose competitive add-on or alternative technologies that interoperate with the goods they buy, because innovators were able to develop and distribute such technologies. But in its current form, the DMCA threatens those freedoms.

The anti-competitive effect of Section 1201 became evident early on with respect to DVDs. The encryption on DVDs was broken almost immediately, as were updated versions. Yet movie studios continued to embrace encryption, using it on every commercial DVD release. Why? One reason is that the movie studios (acting through their agent, the DVD Copy Control Association) could force innovators to sign a license agreement for that encryption software before they built anything that could decrypt a DVD. That, in turn, gave the movie studios unprecedented power to influence the pace and nature of innovation in the world of DVDs. Any new feature (like copying to a hard drive) had to get approved by the 3-way "inter-industry" negotiation (movie studios, incumbent consumer electronics companies, and major computer manufacturers) that is DVD-CCA. In other words, businesses had to get permission (from their adversaries and competitors!) before they could innovate. If these systems had been in place earlier, there would never have been a Betamax videocassette recorder, much less an iPod.

But the problem did not stop with DVD technologies. Most modern durable goods—including household appliances, power tools, calculators, cameras, stereos, printer cartridges, garage door openers, as well as video game controllers, headsets, and memory cards—contain some element of copyrightable software code. In order for replacement parts and compatible accessories to function, they must "access" the code inside. If unauthorized access amounts to circumvention of an access control and is therefore prohibited, the manufacturer can use the DMCA to assert exclusive control over the market for those goods.

The detrimental effects on consumers are well documented. For instance, cell phone manufacturers sell phones equipped with technological protection measures that lock consumers to a particular service provider, forcing them to pay artificially inflated service charges and crippling the market for used phones. According to the claims of major U.S. wireless carriers, unlocking a phone without your carrier's permission violates the DMCA. But a prohibition on unlocking has nothing to do with preventing infringement. Camera makers have similarly installed

technological protection measures that render pictures unreadable in competitors' photo-editing programs, preventing consumers from editing their own photographs with their preferred software.

Similarly, Apple uses technical measures backed by the DMCA to lock iPhone owners into obtaining software ("apps") exclusively from Apple's own iTunes App Store, where Apple must approve every app and retains 30% of revenues generated by app sales. This business practice had significant consequences for both competition and speech, as Apple regularly rejects apps that might compete with Apple's own offerings or that are deemed "potentially offensive."

Responding to intensive efforts, the Librarian of Congress granted an exemption allowing iPhone users to "jailbreak" their phones and install "unapproved" apps, but that exemption is narrow, temporary, and contingent on the Librarian's willingness to renew it every three years.

And that's just the beginning. The DMCA has been used to block aftermarket competition in laser printer toner cartridges, garage door openers, videogame console accessories, and computer maintenance services. For example, StorageTek sells data storage hardware to large enterprise clients. It also sells maintenance services for its products. Custom Hardware is an independent business that repairs StorageTek hardware. In an effort to eliminate this competitor in the maintenance services market, StorageTek sued under the DMCA, arguing that Custom Hardware had circumvented certain passwords designed to block independent service providers from using maintenance software included in the StorageTek hardware systems. In other words, StorageTek was using the DMCA to ensure that its customers had only one place to turn for repair services.

The infamous Lexmark litigation is another case-in-point. Lexmark, the second-largest laser printer maker in the U.S., added authentication routines between its printers and cartridges explicitly to hinder aftermarket toner vendors. Static Control Components (SCC) reverse-engineered these measures and sold "Smartek" chips that enabled refilled cartridges to work in Lexmark printers. Lexmark then used the DMCA to obtain an injunction banning SCC from selling its chips to cartridge remanufacturers. SCC ultimately succeeded in getting the injunction overturned, but only after nineteen months of expensive litigation while its product was held off the market. The litigation alone sent a chilling message to those in the secondary market for Lexmark cartridges.

More recently, Microsoft used the DMCA to try to shut down competition for gaming accessories. Datel, Inc. produces third-party accessories for every major videogame console, including Microsoft's Xbox 360. As with all third-party manufacturers, Datel must engineer its accessories so that they will be compatible with the customer's console; this frequently requires reverse engineering or other work-arounds. In 2009, Microsoft issued a mandatory firmware update for all Xbox 360 consoles connected to the Internet. This update had no effect on Microsoft's own memory cards, but rendered Datel's less expensive memory cards completely unusable. When Datel sued Microsoft for antitrust violations, Microsoft counterclaimed by accusing Datel of violating the DMCA. In a nutshell, Microsoft forced consumers to purchase its own memory cards and then used the DMCA to attack legitimate competitors.

Moreover, manufacturers of ordinary consumer products have sought to extend the DMCA to police any consumer behavior or innovation that is contrary to their preferences. For example,

calculator manufacturers have brought circumvention claims against hobbyists who reverse-engineered their personal graphing calculators to develop alternative operating systems for personal use.

D. Expansions of Copyright Scope in Software

In recent years, technology companies have sought to expand copyright to cover functional software elements and data formats that are needed to create interoperable products.

The most prominent recent example is the Federal Circuit's mistaken decision in *Oracle v. Google*. For decades, computer scientists have relied on the open nature of application programming interfaces (APIs) to enable rapid innovation in computer technology. For decades, circuit courts have supported that reliance, concluding that Section 102(b) of the Copyright Act protects a programmer's source code as creative expression, but does not cover the processes, systems, and methods of operation that code may employ to interface with other software. The district court correctly followed that precedent and rejected Oracle's claim that the Java APIs could be copyrightable. Sadly, the Federal Circuit chose to split with the other circuits and reverse the district court. That decision upended decades of industry practice and threatens the basic principles upon which our technology sector was built.

Compounding the problem, a second decision by the Federal Circuit in the same case held that Google's use of the Java APIs were not fair use, again breaking with precedent from other circuits and overruling a jury determination on a highly fact-specific issue.

Not surprisingly, these Federal Circuit decisions have been harshly criticized. As many commentators have noted, if the Federal Circuit view had been accepted at the birth of modern computing, many important technologies would never have entered the market. For example, the widespread availability of diverse, cheap, and customizable personal computers owes its existence to the lack of copyright on the specification for IBM's Basic Input/Output System (BIOS) for the PC. And open APIs were essential to many modern computing developments, including those of operating systems such as UNIX, programming languages such as C, the Internet's network protocols, and cloud computing.

When programmers can freely reimplement or reverse engineer an API without obtaining a costly license or risking a lawsuit, they can create compatible software that the interface's original creator might never have envisioned or had the resources to develop. Moreover, compatible APIs enable people to switch platforms and services freely, and to find software that meets their needs regardless of what browser or operating system they use. Without the compatibility enabled by the open nature of APIs, consumers could be forced to leave their data and programs behind when they switch to a new service.

The freedom to reimplement APIs also helps developers rescue "orphan" software or data—systems that are no longer supported by their creators. When a popular computer platform or service shuts down, the ability to freely reimplement APIs protects the communities that rely on that software. Government entities and nonprofits are especially susceptible to the orphan programs problem as they often cannot afford to upgrade and are left using legacy technologies for years or decades.

Thus, the Federal Circuit's decision poses a significant threat to the technology sector and to the public. Thanks to that decision, API creators may have veto rights over any developer who wants to create a compatible program—regardless of whether she copies any literal code from the original API implementation.

But the problem is not confined to APIs. Creating drop-down menus that use a similar layout for commands was the subject of copyright litigation (lotus), as was the functional input and output behavior of its interpreter/compiler (SAS) and a standardized collection of software commands (Cisco). And these examples reflect only the pool of technologies that reached actual litigation. The number of technologies threatened with litigation, or chilled out of existence, is far greater.

CONCLUSION

EFF appreciates the Commission's efforts to consider competition policy holistically. Intellectual property laws, along with contract enforcement for digital goods, have an undeniable impact on competition. Future policy recommendations and enforcement actions should account for this impact.

Before the

Federal Trade Commission

Hearings on Competition and Consumer Protection in the 21st Century
Project Number P181201

Comments on Topic 4: The Intersection Between Privacy, Big Data, and Competition

August 17, 2018

Submitted by:
Electronic Frontier Foundation
Bennett Cyphers
Jamie L. Williams
815 Eddy St
San Francisco, CA 94109
(415) 436-9333
bennett@eff.org
jamie@eff.org

The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows. EFF represents over 40,000 dues-paying members, including consumers, hobbyists, artists, computer programmers, entrepreneurs, students, teachers, and researchers.

Increasing market concentration and structural barriers to competition for Internet-related businesses threaten the values of free expression, privacy, and the innovation that has made the Internet a powerful force in daily life. It is imperative that policymakers and industry address competition issues actively and thoughtfully, avoiding approaches that will themselves harm the rights and freedoms of Internet users, or impede innovation.

A. Access to Data—and User Control Over Their Own Data—Is Critical for Competition.

In today's data-driven world, access to data is critical for competition. The web's largest platforms are well aware of this; their companies were built on consumer data. These same companies are now attempting to stop competition by cutting off competitors' access to publicly available data, blocking interoperable technologies, and failing to give users any meaningful ability to transport their data to other platforms. This is a problem. Fostering competition is an important component of the fight for online civil liberties. Consumers suffer when they have to rely on just a few platforms to communicate and learn online, and to protect their rights. Those few, dominant platforms have little incentive to protect user privacy, and sometimes even to maintain robust security practices to protect users, and they often substitute their own view of what constitutes valuable speech for that of their users or the broader public.

Facebook and its subsidiaries, for instance, are over ten times more valuable than the next two largest social media companies outside China—Twitter and Snapchat—combined. The company has cemented its dominance by buying out potential competitors before they've had a chance to grow (like Instagram) and waging wars of attrition against others (like Snapchat) when it can't. Because of its massive reach across much of the world, the platform can effectively censor public speech,[1] perform psychological experiments,[2] and potentially sway elections on the scale of a nation-state. If users don't like the way Facebook wields this power, there is nowhere else as ubiquitous or as well-populated for them to go. Facebook's trove of user data is its most valuable asset, which presents a dilemma. Thanks to network effects,[3] every user who joins a social network makes it more valuable for advertisers and more useful to everyone else. Without some access to the data Facebook has, it is virtually impossible for upstart platforms to compete with the behemoth now used by nearly a third of the world.[4]

To protect consumers and ensure competition in a data-driven world, efforts to maintain monopolistic control over Internet users and their data must be stopped, and Internet users must be given meaningful control of their own data.

B. Protecting Competition Requires New Privacy Laws and Regulations.

Protecting competition—by stopping efforts to maintain monopolistic control over user data and granting users meaningful control of their own data—requires well thought out privacy laws and regulations.

For many years, EFF has urged technology companies, legislators, and regulators to do a better job of giving technology users control over their data and protecting their users' privacy and civil liberties. EFF has, and continues to,[5] pressure the companies themselves, in hopes that mature players would see the importance of implementing real privacy protections. However, where voluntary efforts had failed to protect consumers, well thought out regulation is needed. [6]

---

[1] https://www.onlinecensorship.org/.

[2] https://www.theguardian.com/technology/2014/jul/02/facebook-apologises-psychological-experiments-on-users.

[3] https://www.vox.com/videos/2018/4/11/17226430/facebook-network-effect-video-explainer.

[4] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

[5] *See, e.g.,* https://www.eff.org/deeplinks/2018/07/facing-facebook-data-portability-and-interoperability-are-anti-monopoly-medicine.

[6] *See, e.g.,* https://www.eff.org/deeplinks/2018/08/how-improve-california-consumer-privacy-act-2018.

In particular, we believe new regulations should:

1. Address when and how online services must acquire affirmative user consent before collecting or sharing personal data, particularly where that data is not necessary for the basic operation of the service. Any request for opt-in consent should be easy to understand and should clearly advise the user what data the operator seeks to gather, how the operator will use it, how long the operator will keep it, and with whom the operator will share it. The request should be renewed any time the operator wishes to use or share data in a new way or gather a new kind of data. And the user should be able to withdraw consent, including for particular purposes.

2. Create an affirmative "right to know" so that users can learn what personal data companies have gathered about them, where they got it, and with whom these companies have shared it (including the government).

3. Create an affirmative right to data access and "data portability," so users can get a complete copy of their data from a service provider and move it to a different platform. The data should be easy to understand, machine-readable, and available in widely-adopted standard formats when applicable.

4. Create new mechanisms for users to hold companies accountable for data breaches and other privacy failures. Companies that suffer data breaches should have to report the breaches to the public in a timely manner. In cases where a breach was caused by inadequate security practices, it should be easier for the people harmed—including those suffering non-financial harms—to take negligent companies to court.

Any new regulations must be judicious and narrowly tailored. Overly burdensome regulation and technology mandates can stifle innovation, especially by small companies. If regulations are too byzantine, only the largest corporations will be able to comply, and the regulations themselves will act as a barrier to entry for smaller competitors. To that end, policymakers should consider tailoring new obligations based on the size of the service in question, taking into account revenue, number of employees, number of users, and other factors.

There are many other considerations to take into account when drafting new privacy rules for the digital economy. For example, policymakers should consider whether and how the rights and obligations they create can be waived, especially where users and companies have unequal bargaining power, such as when a user is prompted to agree to dozens of pages of terms before using a service. Privacy regulations must be balanced against First Amendment interests. For example, the "right to know" should extend to data a newspaper's website has collected about a user's browsing habits, but must not cover a reporter's investigative file. And at every step, policymakers should consult with data experts so they understand what data can be collected and used, under what circumstances.

There are few easy answers in privacy regulation, and no new regulation will ever be a panacea. Still, we believe the stakes are too high for inaction. We hope the Commission will use the powers at its disposal, including its Section 5 authority and sound recommendations to Congress, to advance sensible, user-friendly privacy laws and regulations.

C. Protecting Competition Also Requires Stopping Efforts by Major Internet Platforms to Use Computer Crime Statutes to Maintain Monopolistic Control Over Data.

New legislation is not enough. To ensure competition in a digital age, we must also put an end to efforts to abuse existing laws to maintain monopolistic control over user data.

Specifically, major Internet companies are currently attempting to co-opt a notoriously imprecise, per-Internet criminal anti-"hacking" statute intended to target computer break-ins, the Computer Fraud and Abuse Act ("CFAA"), and their state law equivalents, and transform these laws into tools for conducting anti-competitive behavior under the color of the law.[7] To protect competition, abuse of the CFAA must stop.

Congress passed the CFAA—which has been dubbed the "worst law in technology"[8]—in 1986, in response to a series of malicious computer break-ins. The law makes it a crime to access a computer "without authorization" but fails to tell us what that means. This vague language has enabled the law to metastasize in some jurisdictions from a law meant to target malicious "hacking" of private computer systems, into a tool for companies and websites to selectively enforce their computer use preferences and policies—such as terms of service prohibitions on using automated web browsing tools to access information—against competitors.

Platforms have taken advantage of this in a number of ways. In recent years, large companies—including Microsoft-owned LinkedIn[9]—have amped up efforts to use the CFAA's civil enforcement provision to punish competitors for using commonplace automated web browsing tools to access information they've published publicly online for the rest of the world to see. As USC Gould Law Professor Orin Kerr has explained, however, posting information publicly on the web and then telling someone they are not authorized to access it is "like publishing a newspaper but then forbidding someone to read it."[10] This is a clear abuse of a law meant to target criminals.

Automated web browsing—also referred to as "web scraping"[11]—is the process of using a computer script to send tailored queries to websites to retrieve specific pieces of content. The technique is used across the web for countless applications, such as aggregating information from multiple sources and identifying and extracting data for analysis.

---

[7] *See generally* Jamie L. Williams, *Automation is Not "Hacking": Why Courts Must Reject Attempts to Use the CFAA as an Anti-Competitive Sword*, 24 B.U. J. Sci. & Tech. L. X (forthcoming 2018).

[8] https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology.

[9] https://www.eff.org/deeplinks/2017/08/judge-cracks-down-linkedins-shameful-abuse-computer-break-law.

[10] *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1169 (2016).

[11] https://www.eff.org/deeplinks/2018/04/scraping-just-automated-access-and-everyone-does-it.

The web is the largest, ever-growing data source on the planet. It's a critical resource for journalists, academics, businesses, and everyday people alike. Meaningful access sometimes requires the assistance of technology, to automate and expedite an otherwise tedious process of accessing, collecting and analyzing public information. As a technical matter, web scraping is simply machine automated web browsing. There is nothing that can be done with a web scraper that cannot be done by a human with a web browser. As one district court judge recently recognized, Web scraping "is merely a technological advance that makes information collection easier; it is not meaningfully different from using a tape recorder instead of taking written notes, or using the panorama function on a smartphone instead of taking a series of photos from different positions."[12]

Use of automated web browsing can help competition by lowering startup information barriers[13] and enable consumers to find deals and discounts online.[14] It can also help uncover unfair or deceptive business practices. ProPublica, for example, used automated web browsing to uncover that Amazon's pricing algorithm was hiding the best deals from its customers.[15] And because broader access to datasets can help correct bias in how algorithms are currently trained, it can also help identify and correct issues of algorithmic bias.[16]

It is important to understand that web scraping is a *widely used* method of interacting with the content on the web: everyone does it—even (and especially) the companies trying to convince courts to punish others for the same behavior. Companies use automated web browsing products to gather web data for a wide variety of uses. [17] Some examples from industry include manufacturers tracking the performance ranking of products in the search results of retailer websites, companies monitoring information posted publicly on social media to keep tabs on issues that require customer support, and businesses staying up to date on news stories relevant to their industry across multiple sources. E-commerce businesses use automated web browsing to monitor competitors' pricing and inventory, and to aggregate information to help manage supply chains. Businesses also use automated web browsers to monitor websites for fraud, perform due diligence checks on their customers and suppliers, and to collect market data to help plan for the future. Gartner has even recommended that all businesses treat the web as their largest data source and predicts that the ability to compete in the digital economy will depend on the ability

---

[12] *Sandvig v. Sessions*, No. CV 16-1368 (JDB), 2018 WL 1568881, at *7 (D.D.C. Mar. 30, 2018).

[13] *See* Rory Van Loo, *Rise of the Digital Regulator*, 66 Duke L.J. 1267, 1285–89 (2017).

[14] *See* Complaint, Sw. Airlines Co. v. Roundpipe LLC, No. 3:18-CV-33 (N.D. Tex. filed Jan. 5, 2018) (lawsuit by Southwest Airlines against a company that used automated web browsing software to enable customers to check flight prices and take advantage of the airline's own rebooking deals).

[15] https://www.propublica.org/article/how-we-analyzed-amazons-shopping-algorithm.

[16] *See* Amanda Levendowski, *How Copyright Law Can Fix AI' s Implicit Bias Problem*, 93 Wash. L. Rev. (forthcoming 2018).

[17] https://www.import.io/post/13-ways-use-web-scraping-tools/.

to curate and leverage web data: "Your company's biggest database isn't your . . . internal database. Rather it's the Web itself."[18]

Even the very companies trying to misuse the CFAA to punish competitors for using automated web browsing tools have used—and continue to use—these same techniques to build their businesses.[19]

Boston University Law Professor Andrew Sellars recently analyzed the sixty-one opinions generated via web scraping cases in the last twenty years. He reported that the "vast majority of these opinions concern claims brought by direct commercial competitors or companies in closely adjacent markets to each other."[20] The CFAA is first and foremost a criminal statute. The fact that these unauthorized Web scraping cases are *consistently* about blocking competition—and not about punishing criminals for breaking into private computer systems—demonstrates that the law is clearly being abused.

The companies seeking to abuse the CFAA in this way are subverting the web's open access norms.[21] These short-sighted and opportunistic efforts threaten open access to information across the Internet, including by investigative journalists, researchers, academics, and individual consumers. And in an era of algorithms and artificial intelligence, lack of access to data is a barrier to product innovation and competition.

LinkedIn, one company involved in recent web scraping litigation, characterizes its reliance on the CFAA as about protecting user privacy, not about stifling competition.[22] But the company's proposed rule—imposing criminal CFAA liability for automated access of publicly available user data by competitors that LinkedIn has told to "go away"—will not truly protect the privacy interests of LinkedIn users who decide to publish their information publicly online. The data will still be freely available on the Web for anyone else to access and use, without consequence. LinkedIn's privacy policy acknowledges the inherent lack of privacy in data users post publicly on its site and makes no promises to users about LinkedIn's ability to protect it:

---

[18] https://www.forbes.com/sites/gartnergroup/2015/02/12/gartner-predicts-three-big-data-trends-for-business-intelligence/.

[19] Microsoft-owned LinkedIn, for example, one company seeking to use the CFAA to block automated Web scraping by a competing service, acknowledges in its privacy policy that it uses automated tools, *i.e.*, Web scraping, to "collect public information about you, such as professional-related news and accomplishments" and makes that information available on its own website—unless a user opts out via adjusting their default privacy settings. *See* LinkedIn, Privacy Policy, §§ 1.1-1.2 (effective May 8, 2018), https://www.linkedin.com/legal/privacy-policy.

[20] *See* Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. Sci. & Tech. L. 424, X (forthcoming 2018) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3221625).

[21] *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1162–64 (2016).

[22] See *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1106 (N.D. Cal. 2017).

"Please do not post or add personal data to your profile that you would not want to be publicly available."[23] What is needed to protect privacy is comprehensive, thoughtful privacy regulation that LinkedIn, its parent company Microsoft, and all other websites and Internet service providers would be subject to.[24]

Platforms have also used the CFAA to go after companies for creating interoperable software and shut down follow-on innovation. Social media giant Facebook, for example, for a decade has pursued litigation against a company that tried back in 2008 to provide a social media aggregation service for users of Facebook and other social media platforms.[25] This service, had it not been stifled in the cradle, could have been a great boon to those who often switch between services like Facebook, LinkedIn, and Twitter, or who struggle to remember who's a friend, who's a contact, and who's a follower, or where they received any given message. Facebook sent the company, Power Ventures, a cease and desist letter and set up an ineffective IP address block. When Power continued to provide its social media aggregation services to Facebook users, Facebook turned to the CFAA. In order to provide its aggregation services, Power Ventures had used—with permission—the valid Facebook login credentials of its users. Facebook claimed that Power Ventures had violated the CFAA by continuing to use these valid credentials after receipt of the cease and desist letter. And in 2016, it convinced the Ninth Circuit to go along with this theory of liability. At Facebook's urging, the court contorted previously clear CFAA precedent and opened the door for even more abuse of the CFAA,[26] including many of the pending automated web browsing cases that are threatening competition and open access across the web today (which consistently rely on the Ninth Circuit's decision in this case).

D. Mergers Involving Data from Third-Party Trackers—Including User Location Data—Must Receive Special Scrutiny.

Finally, to protect both competition and consumers, merging of rich first-party datasets with *third-party trackers*—systems that use ads and other third-party plugins to track user habits around the web and on mobile devices—must receive special scrutiny. Such mergers present privacy risks to users and exacerbate existing network effects and make it difficult for companies without comparable datasets to compete.

In 2007, Google purchased Doubleclick, a third-party advertising and tracking company. The merger was reviewed by the Commission at the time, and the majority determined that the competition and privacy concerns were not sufficient to challenge the acquisition. In 2013, Facebook acquired a similar product, Atlas, from Microsoft, which they have since folded into their own brands.

---

[23] See LinkedIn, Privacy Policy, § 1.1 (effective May 8, 2018), https://www.linkedin.com/legal/privacy-policy.

[24] *See* Section B, *supra*.

[25] https://www.eff.org/cases/facebook-v-power-ventures.

[26] https://www.eff.org/deeplinks/2016/12/take-two-ninth-circuit-revises-two-password-sharing-decisions-fails-fix-cfaa-mess.

Today, Facebook's and Google's tracking networks are the two largest on the English-speaking Internet by far. Facebook tracking code, including social plugins and its invisible "pixel," is present on nearly 25% of the top one million sites on the Internet. The company's ad network also covers 40% of the top 500 most popular mobile apps. By some metrics, Google's reach is even broader. Rich tracking code for Doubleclick is present on over 20% of the top million sites; including Google Analytics and other services, code from Google is present on approximately three quarters of sites on the web.

In addition to their third-party tracking capabilities, both of these companies have massive first-party data stores. That gives them the ability to link data from their third party trackers with the data that users have provided them voluntarily, including real names, demographic data, contacts, communication, and interests.

We believe these kinds of mergers and acquisitions raise both privacy and competition concerns.

From a privacy perspective, mergers between tracking companies and first-party data stores create risks to users that are not present in their component parts. Normally, third-party tracking companies creates anonymous, ad-hoc profiles for users as they browse the web. They have difficulty linking one user's activity across different devices, and when a user clears cookies or switches to a new browser, the tracking company may have to start building a new profile from scratch. However, when a Facebook user browses the web, their activity can be immediately and permanently linked to their Facebook identity via Facebook's cookies. When a user uploads a photo or comments on a friend's post, they implicitly consent to giving the company their data. But when they leave facebook.com to browse the web, they may not realize that Facebook is *still tracking them*. Even if they do, the company offers no way to opt out of that collection or to delete the data after the fact. The result is a potent, permanent profile of that user's digital life, combining data they have chosen to share with data collected surreptitiously while they might have felt anonymous.

From a competition perspective, the mergers exacerbate existing network effects and make it difficult for companies without comparable datasets to compete. They give the companies competitive advantages for both their first-party platforms and third-party advertising products. Facebook touts their ability to advertise to "real people"—that is, to use information from Facebook profiles to target individuals outside of Facebook products. Third-party ad platforms that do not possess a similar first-party dataset cannot hope to do the same. Furthermore, these companies have a privileged view of the landscape of the Internet, and therefore of their competition. This gives some companies "a relative advantage in accessing and analyzing data to discern threats well before others, including the government."[27]

There are some behavioral remedies that we believe could mitigate the harms of these mergers. After acquiring Doubleclick, Google volunteered to keep the data it collected through

[27] *See* Maurice E. Stucke, *Should We Be Concerned About Data-opolies?*, 2 Geo. L. Tech. Rev. 275, 305 (2018) (available at https://ssrn.com/abstract=3144045 or http://dx.doi.org/10.2139/ssrn.3144045).

Doubleclick separate from the rest of its user data. Commissioner Harbour, in her dissenting statement for the investigation, predicted that the company would eventually reverse this policy, and in 2016, it did. Today, it might make sense to enforce a similar policy: require that data from third-party tracking networks must be "siloed" away from first-party data so that anonymous web activity cannot be linked to rich digital identities.

Finally, we believe traditional metrics for assessing these mergers are insufficient, and new means of evaluation are needed in the future. In her dissent, Commissioner Harbour wrote, "Traditional competition analysis of Google's acquisition of DoubleClick fails to capture the interests of all the relevant parties." We agree, and we believe that mergers between data collectors should be scrutinized more strictly than they have in the past, and on more comprehensive grounds. We hope to engage in an ongoing conversation about how to assess competitive harms caused by consolidation in the age of big data.

Before the

Federal Trade Commission

Hearings on Competition and Consumer Protection in the 21st Century
Project Number P181201

Comments on Topic 3: The Identification and Measurement of Market Power and Entry Barriers, and the Evaluation of Collusive, Exclusionary, or Predatory Conduct or Conduct that Violates the Consumer Protection Statutes Enforced by the FTC, in Markets Featuring "Platform" Businesses

August 20, 2018

Submitted by:
Electronic Frontier Foundation
Bennett Cyphers
Jamie L. Williams
815 Eddy St
San Francisco, CA 94109
(415) 436-9333
bennett@eff.org
jamie@eff.org

The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows. EFF represents over 40,000 dues-paying members, including consumers, hobbyists, artists, computer programmers, entrepreneurs, students, teachers, and researchers.

Increasing market concentration and structural barriers to competition for Internet-related businesses threaten the values of free expression, privacy, and the innovation that has made the Internet a powerful force in daily life. It is imperative that policymakers and industry address competition issues actively and thoughtfully, avoiding approaches that will themselves harm the rights and freedoms of Internet users, or impede innovation.

A. Lack of Access to Data—and Lack of User Control Over Data—Is an Entry Barrier in Markets Featuring Platform Businesses.

In today's data-driven world, access to data is critical for competition—particularly in markets featuring platform businesses and social networks. The web's largest platforms are well aware of this; their companies were built on consumer data. These same companies are now attempting to stop competition by cutting off competitors' access to publicly available data, blocking interoperable technologies, and failing to give users any meaningful ability to transport their data to other platforms. This is a threat to competition.

Facebook and its subsidiaries, for example, are over ten times more valuable than the next two largest social media companies outside China—Twitter and Snapchat—combined. The social media giant has cemented its dominance by buying out potential competitors before they've had a chance to grow (like Instagram) and waging wars of attrition against others (like Snapchat) when it can't. Because of its massive reach across much of the world, the platform can effectively censor public speech,[1] perform psychological experiments,[2] and potentially sway elections on the scale of a nation-state. If users don't like the way Facebook wields this power, there is nowhere else as ubiquitous or as well populated for them to go. Facebook's trove of user data is its most valuable asset, which presents a dilemma. Thanks to ***network effects***,[3] every user who joins a social network makes it more valuable for advertisers and more useful to everyone else. Without some access to the data Facebook has, it is virtually impossible for upstart platforms to compete with the behemoth now used by nearly a third of the world.[4]

To protect consumers and ensure competition in a data-driven world, two things are needed.

First, Internet users must be given meaningful control of their own data. They must have an affirmative right to data access and "data portability," so they can get a complete copy of their data from a service provider and move it to a different platform. The data should be easy to understand, machine-readable, and available in widely adopted standard formats when applicable.

Second, the Commission must take into account efforts by large platforms to maintain monopolistic control over Internet users and their data in its analysis of competition and consumer protection issues. Such behavior is predatory and exclusionary, and a threat not only to competition, but also to consumers' online civil liberties. Consumers suffer when they have to rely on just a few platforms to communicate and learn online, and to protect their rights. Those few, dominant platforms have little incentive to protect user privacy, and sometimes even to maintain robust security practices to protect users, and they often substitute their own view of what constitutes valuable speech for that of their users or the broader public.

B. Major Internet Platforms Are Using Computer Crime Statutes to Maintain Monopolistic Control Over Data and to Conduct Exclusionary and Predatory Behavior Under Color of the Law.

One area of exclusionary and predatory conduct the Commission should pay careful attention to is large platforms abusing existing laws to maintain monopolistic control over user data. Specifically, major Internet companies are currently attempting to co-opt a notoriously

---

[1] https://www.onlinecensorship.org/.

[2] https://www.theguardian.com/technology/2014/jul/02/facebook-apologises-psychological-experiments-on-users.

[3] https://www.vox.com/videos/2018/4/11/17226430/facebook-network-effect-video-explainer.

[4] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

imprecise, pre-Internet criminal anti-"hacking" statute intended to target computer break-ins, the Computer Fraud and Abuse Act ("CFAA"), and their state law equivalents, and transform these laws into tools for conducting anti-competitive behavior under the color of the law.[5] To protect comptition, abuse of the CFAA must stop.

Congress passed the CFAA—which has been dubbed the "worst law in technology"[6]—in 1986, in response to a series of malicious computer break-ins. The law makes it a crime to access a computer "without authorization" but fails to tell us what that means. This vague language has enabled the law to metastasize in some jurisdictions from a law meant to target malicious "hacking" of private computer systems, into a tool for companies and websites to selectively enforce their computer use preferences and policies—such as terms of service prohibitions on using automated web browsing tools to access information—against competitors.

Platforms have taken advantage of this in a number of ways. In recent years, large companies—including Microsoft-owned LinkedIn[7]—have amped up efforts to use the CFAA's civil enforcement provision to punish competitors for using commonplace automated web browsing tools to access information they've published publicly online for the rest of the world to see. As USC Gould Law Professor Orin Kerr has explained, however, posting information publicly on the web and then telling someone they are not authorized to access it is "like publishing a newspaper but then forbidding someone to read it."[8] This is a clear abuse of a law meant to target criminals.

Automated web browsing—also referred to as "web scraping"[9]—is the process of using a computer script to send tailored queries to websites to retrieve specific pieces of content. The technique is used across the web for countless applications, such as aggregating information from multiple sources and identifying and extracting data for analysis.

The web is the largest, ever-growing data source on the planet. It's a critical resource for journalists, academics, businesses, and everyday people alike. Meaningful access sometimes requires the assistance of technology, to automate and expedite an otherwise tedious process of accessing, collecting and analyzing public information. As a technical matter, web scraping is simply machine automated web browsing. There is nothing that can be done with a web scraper that cannot be done by a human with a web browser. As one district court judge recently recognized, web scraping "is merely a technological advance that makes information collection easier; it is not meaningfully different from using a tape recorder instead of taking written notes,

---

[5] *See generally* Jamie L. Williams, *Automation is Not "Hacking": Why Courts Must Reject Attempts to Use the CFAA as an Anti-Competitive Sword*, 24 B.U. J. Sci. & Tech. L. X (forthcoming 2018) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3234076).

[6] https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology.

[7] https://www.eff.org/deeplinks/2017/08/judge-cracks-down-linkedins-shameful-abuse-computer-break-law.

[8] *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1169 (2016).

[9] https://www.eff.org/deeplinks/2018/04/scraping-just-automated-access-and-everyone-does-it.

or using the panorama function on a smartphone instead of taking a series of photos from different positions."[10]

Use of automated web browsing can help competition by lowering startup information barriers[11] and enable consumers to find deals and discounts online.[12] It can also help uncover unfair deceptive business practices. ProPublica, for example, used automated web browsing to uncover that Amazon's pricing algorithm was hiding the best deals from its customers.[13] And because broader access to datasets can help correct bias in how algorithms are currently trained, it can also help identify and correct issues of algorithmic bias.[14]

It is important to understand that web scraping is a *widely used* method of interacting with the content on the web: everyone does it—even (and especially) the companies trying to convince courts to punish others for the same behavior. Companies use automated web browsing products to gather web data for a wide variety of uses.[15] Some examples from industry include manufacturers tracking the performance ranking of products in the search results of retailer websites, companies monitoring information posted publicly on social media to keep tabs on issues that require customer support, and businesses staying up to date on news stories relevant to their industry across multiple sources. E-commerce businesses use automated web browsing to monitor competitors' pricing and inventory, and to aggregate information to help manage supply chains. Businesses also use automated web browsers to monitor websites for fraud, perform due diligence checks on their customers and suppliers, and to collect market data to help plan for the future. Gartner has even recommended that all businesses treat the web as their largest data source and predicts that the ability to compete in the digital economy will depend on the ability to curate and leverage web data: "Your company's biggest database isn't your . . . internal database. Rather it's the Web itself."[16]

---

[10] *Sandvig v. Sessions*, No. CV 16-1368 (JDB), 2018 WL 1568881, at *7 (D.D.C. Mar. 30, 2018).

[11] *See* Rory Van Loo, *Rise of the Digital Regulator*, 66 Duke L.J. 1267, 1285–89 (2017).

[12] *See* Complaint, *Sw. Airlines Co. v. Roundpipe LLC*, No. 3:18-CV-33 (N.D. Tex. filed Jan. 5, 2018) (lawsuit by Southwest Airlines against a company that used automated web browsing software to enable customers to check flight prices and take advantage of the airline's own rebooking deals).

[13] https://www.propublica.org/article/how-we-analyzed-amazons-shopping-algorithm.

[14] *See* Amanda Levendowski, *How Copyright Law Can Fix AI' s Implicit Bias Problem*, 93 Wash. L. Rev. (forthcoming 2018).

[15] https://www.import.io/post/13-ways-use-web-scraping-tools/.

[16] https://www.forbes.com/sites/gartnergroup/2015/02/12/gartner-predicts-three-big-data-trends-for-business-intelligence/.

Even the very companies trying to misuse the CFAA to punish competitors for using automated web browsing tools have used—and continue to use—these same techniques to build their businesses.[17]

Boston University Law Professor Andrew Sellars recently analyzed the sixty-one opinions generated via web scraping cases in the last twenty years. He reported that the "vast majority of these opinions concern claims brought by direct commercial competitors or companies in closely adjacent markets to each other."[18] The CFAA is first and foremost a criminal statute. The fact that these unauthorized Web scraping cases are *consistently* about blocking competition—and not about punishing criminals who break into private computer systems—demonstrates that the law is clearly being abused.

The companies seeking to abuse the CFAA in this way are subverting the web's open access norms.[19] These short-sighted and opportunistic efforts threaten open access to information across the Internet, including by investigative journalists, researchers, academics, and individual consumers. And in an era of algorithms and artificial intelligence, lack of access to data is a barrier to product innovation.

LinkedIn characterizes its reliance on the CFAA as about protecting user privacy, not about stifling competition.[20] But the company's proposed rule—imposing criminal CFAA liability for automated access of publicly available user data by competitors that LinkedIn has told to "go away"—will not truly protect the privacy interests of LinkedIn users who decide to publish their information publicly online. The data will still be freely available on the web for anyone else to access and use, without consequence. LinkedIn's privacy policy acknowledges the inherent lack of privacy in data users post publicly on its site and makes no promises to users about LinkedIn's ability to protect it: "Please do not post or add personal data to your profile that you would not want to be publicly available."[21] What is needed to protect privacy is

---

[17] Microsoft-owned LinkedIn, for example, one company seeking to use the CFAA to block automated Web scraping by a competing service, acknowledges in its privacy policy that it uses automated tools, *i.e.*, Web scraping, to "collect public information about you, such as professional-related news and accomplishments" and makes that information available on its own website—unless a user opts out via adjusting their default privacy settings. *See* LinkedIn, Privacy Policy, §§ 1.1-1.2 (effective May 8, 2018), https://www.linkedin.com/legal/privacy-policy.

[18] *See* Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. Sci. & Tech. L. 424, X (forthcoming 2018) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3221625).

[19] *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1162–64 (2016) (available at https://columbialawreview.org/content/norms-of-computer-trespass/).

[20] See *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1106 (N.D. Cal. 2017).

[21] See LinkedIn, Privacy Policy, § 1.1 (effective May 8, 2018), https://www.linkedin.com/legal/privacy-policy.

comprehensive, thoughtful privacy regulation that LinkedIn, its parent company Microsoft, and all other websites and Internet service providers would be subject to.[22]

Platforms have also used the CFAA to go after companies for creating interoperable software and to shut down follow-on innovation. Social media giant Facebook, for example, for a decade has pursued litigation against a company that tried back in 2008 to provide a social media aggregation service for users of Facebook and other social media platforms.[23] This service, had it not been stifled in the cradle, could have been a great boon to those who often switch between services like Facebook, LinkedIn, and Twitter, or who struggle to remember who's a friend, who's a contact, and who's a follower, or where they received any given message. Facebook sent the company, Power Ventures, a cease and desist letter and set up an ineffective IP address block. When Power continued to provide its social media aggregation services to Facebook users, Facebook turned to the CFAA. In order to provide its aggregation services, Power Ventures had used—with permission—the valid Facebook login credentials of its users. Facebook claimed that Power Ventures had violated the CFAA by continuing to use these valid credentials after receipt of the cease and desist letter. And in 2016, it convinced the Ninth Circuit to go along with this theory of liability. At Facebook's urging, the court contorted previously clear CFAA precedent and opened the door for even more abuse of the CFAA,[24] including many of the pending automated web browsing cases that are threatening competition and open access across the web today (which consistently rely on this Ninth Circuit decision).

C. Because Data Is a Measure of Market Power, Mergers Involving Data from Third-Party Trackers—Including User Location Data—Must Receive Special Scrutiny.

Finally, to protect both competition and consumers, merging of rich first-party datasets with *third-party trackers*—systems that use ads and other third-party plugins to track user habits around the web and on mobile devices—must receive special scrutiny. Such mergers present privacy risks to users and exacerbate existing network effects, and they make it difficult for companies without comparable datasets to compete.

In 2007, Google purchased Doubleclick, a third-party advertising and tracking company. The merger was reviewed by the Commission at the time, and the majority determined that the competition and privacy concerns were not sufficient to challenge the acquisition. In 2013, Facebook acquired a similar product, Atlas, from Microsoft, which they have since folded into their own brands.

Today, Facebook and Google's tracking networks are the two largest on the English-speaking Internet by far. Facebook tracking code, including social plugins and its invisible

---

[22] *See, e.g.*, https://www.eff.org/deeplinks/2018/08/how-improve-california-consumer-privacy-act-2018; *see also* EFF Comments submitted in response to Topic #4 (FTC_P181201), Sec. B.

[23] https://www.eff.org/cases/facebook-v-power-ventures.

[24] https://www.eff.org/deeplinks/2016/12/take-two-ninth-circuit-revises-two-password-sharing-decisions-fails-fix-cfaa-mess.

"pixel," is present on nearly 25% of the top one million sites on the Internet. The company's ad network also covers 40% of the top 500 most popular mobile apps. By some metrics, Google's reach is even broader. Rich tracking code for Doubleclick is present on over 20% of the top million sites; including Google Analytics and other services, code from Google is present on approximately three quarters of sites on the web.

In addition to their third-party tracking capabilities, both of these companies have massive first-party data stores. That gives them the ability to link data from their third party trackers with the data that users have provided them voluntarily, including real names, demographic data, contacts, communication, and interests.

We believe these kinds of mergers and acquisitions raise both privacy and competition concerns.

From a privacy perspective, mergers between tracking companies and first-party data stores create risks to users that are not present in their component parts. Normally, third-party tracking companies creates anonymous, ad-hoc profiles for users as they browse the web. They have difficulty linking one user's activity across different devices, and when a user clears cookies or switches to a new browser, the tracking company may have to start building a new profile from scratch. However, when a Facebook user browses the web, their activity can be immediately and permanently linked to their Facebook identity via Facebook's cookies. When a user uploads a photo or comments on a friend's post, they implicitly consent to giving the company their data. But when they leave facebook.com to browse the web, they may not realize that Facebook is *still tracking them*. Even if they do, the company offers no way to opt out of that collection or to delete the data after the fact. The result is a potent, permanent profile of that user's digital life, combining data they have chosen to share with data collected surreptitiously while they might have felt anonymous.

From a competition perspective, *these mergers exacerbate existing network effects* and make it difficult for companies without comparable datasets to compete. They give the companies competitive advantages for both their first-party platforms and third-party advertising products. Facebook touts their ability to advertise to "real people"—that is, to use information from Facebook profiles to target individuals outside of Facebook products. Third-party ad platforms that do not possess a similar first-party dataset cannot hope to do the same. Furthermore, these companies have a privileged view of the landscape of the Internet, and therefore of their competition. This gives some companies "a relative advantage in accessing and analyzing data to discern threats well before others, including the government."[25]

There are some behavioral remedies that we believe could mitigate the harms of these mergers. After acquiring Doubleclick, Google volunteered to keep the data it collected through Doubleclick separate from the rest of its user data. Commissioner Harbour, in her dissenting statement for the investigation, predicted that the company would eventually reverse this policy,

[25] *See* Maurice E. Stucke, *Should We Be Concerned About Data-opolies?*, 2 Geo. L. Tech. Rev. 275, 305 (2018) (available at https://ssrn.com/abstract=3144045 or http://dx.doi.org/10.2139/ssrn.3144045).

and in 2016, it did. Today, it might make sense to enforce a similar policy: require that data from third-party tracking networks must be "siloed" away from first-party data so that anonymous web activity cannot be linked to rich digital identities.

Finally, we believe traditional metrics for assessing these mergers are insufficient, and new means of evaluation are needed in the future. In her dissent, Commissioner Harbour wrote, "Traditional competition analysis of Google's acquisition of DoubleClick fails to capture the interests of all the relevant parties." We agree, and we believe that mergers between data collectors should be scrutinized more strictly than they have in the past, and on more comprehensive grounds. We hope to engage in an ongoing conversation about how to assess competitive harms caused by consolidation in the age of big data.