University of Pittsburgh

The Right to Digital Privacy

A Right Opposed by Right-Wing Politics

Dalton Scharff

CS 0590: Social Implications of Computing Technology

Professor Quirin

12 April 2017

The Right to Digital Privacy

On Monday, April 3, President Donald Trump signed S.J.Res.34, forbidding the Federal Communications Commission (FCC) from enacting any law that would limit an internet service provider (ISP) from selling its users’ personal data to private companies. Now Public Law 115-22, S.J.Res.34 was first introduced to the United States Senate in response the FCC’s rules to prevent ISPs from selling user data, which was set to go into effect on December 4, 2017 (Klosowski). To summarize, this recently passed law has no immediate effect on the average internet consumer. One might then wonder why this recently passed law is so important and deserving of the bipartisan outcry it is receiving. When a country revokes an implicit right from its citizens, it should do so for the wellbeing of the public. Public Law 115-22 revokes a right, but neglects to take into consideration the interest of the individual while reminding us of the power that unelected lobbyists have over our government leaders. The right to digital privacy is an important one that affects all internet users, and allowing ISPs to sell user data not only violates this right, but also sets a precedent for security of future technologies.

**The Negative Effects**

If you have ever been shopping online for shoes and later see shoe related ads in YouTube videos or next to your Facebook feed, then your internet user data has already been collected and sold. This has been happening for years by companies known as ‘data brokers’, with the information they collect often called ‘big data’. The corporations in this multi-billion-dollar industry collect information on each user by tracking visited websites, form fields, and even how long a webpage is viewed. This data is then analyzed and sold so that content (i.e., advertisements) can be fine-tuned to match that user’s interests (“Data Broker Opt-Out List”). The Federal Trade Commission (FTC) has set the precedence on the legality of this, as they note that a user’s personal data can be collected and traded only if it is received only by those with “permissible purpose”, a phrase that seems intentionally vague (Cackley 5).

While the FTC hopes to push data brokers toward having a more transparent data collection process, they are not the ones that many of us should be worried about. Data collection companies only operate on websites that give these companies consent. Many of the websites we frequent do sell our information, as that is how sites like Facebook create revenue while not charging the user. However, a user has the choice to visit these websites, and by visiting these sites, agrees to their terms of service which should state what data is being collected. With ISPs on the other hand, many Americans do not have a choice between providers. Companies such as Comcast and Time Warner Cable, two of the biggest players in the internet providing game, work together so that their coverage areas do not overlap. This means that if my ISP, the only one that will provide me service, chooses to sell its users’ data, I must either agree or go without internet (Tarnoff). With the United Nations declaring that internet access as a basic human right, this would be a choice of rescinding my right to internet or my right to privacy (Kravets).

Currently, it seems that no ISPs are ready to sell the entirety of your data just yet. However, Xfinity, Comcast’s internet service division, states in their privacy policy that they do currently sell “non-personally-identifiable information”, that is, data without your name attached, to companies to help “improve [their] services.” This means that they have been and continue to collect your data, but do not sell it with your name attached. Therefore, data brokers cannot add this information to a user’s individual profile. When they decide to make the switch to selling data with identifying information, all that old data without identifying information can be resold with your name attached, leaving your whole internet history up for grabs (Tarnoff).

This begs the question, since ISPs are legally allowed to sell identifiable user data and have been since the beginning, why have they not? Prior to Public Law 115-22, the matter of ISPs selling user data was a legal grey area. Therefore, ISPs cautiously nudged the boundaries, selling data without personal identification. Now, they are in the clear to do so, but while this law is still in the public eye, no company dares to be the first to make the switch. Once attention falls away and one company makes the change to their policy, all others will follow suit, as it will create even more revenue for these businesses that we already pay for their service (Tarnoff).

Who cares if ISPs make a bit more money and you get ads based on things you are interested in? You should. Unlike data miners who utilize popular sites like Google and Facebook to gather information, your ISP sees all your internet traffic, and has had the ability to track you since the first time you ever logged on (Tarnoff). Tim Sparapani, a privacy lawyer for the American Civil Liberties Union, states that the private companies who have already been data mining are not just learning your interests, they are creating complete dossiers on individual users. Sparapani explains that these companies know whether you suffer from alcoholism, depression, psychiatric or genetic problems, and many more personal statistics that you may wish to keep a secret. The largest data broker, Acxiom, brags that it stores on average 1,500 facts on more than two-thirds of all Americans. ISPs can know even more than this, since they can track every single click or keystroke you make on the web (Kroft).

In addition to collecting very personal information, data mining is also a lucrative business. During just one year, Facebook makes over eight dollars per user just by selling user data. Across Facebook’s nearly two billion monthly users, that comes to about sixteen billion dollars (Bolluyt). Your ISP can know even more about each of its users than Facebook, and everyone using the internet must go through an ISP, so just imagine how much money this will make the companies. Even though no ISPs are currently selling data, and Comcast says that it has “no plans” to sell browsing history, this does not mean it will not change (Goel and Narayanan). Comcast regularly ranks at the bottom of the American Consumer Satisfaction Index, surrounded by other service providers. These businesses often do not focus on meeting the requests of the consumer, but rather solely aim for higher profit margins (Tarnoff). Along with all the other fees that come with paying for internet service, companies could now charge more if the customer would like to keep his or her data private. In 2013, AT&T experimented with charging customers an extra $29 so their browsing data would not be sold. This continued until the FCC, the same commission now deemed powerless on this front, warned the company against this practice (Brodkin). So, this had happened in the past, and we should expect to see history repeat itself in the coming months.

The true fear that drives the outrage behind this bill being passed is not that the data is being collected or that big companies are growing even larger, it is the personal damage that this data could cause if it were to fall into the wrong hands. The dossiers that data brokers create are not necessarily correct. For example, if someone is doing research on gambling addiction, this does not mean they are a gambling addict. They could be a psychologist gathering information. Yet, if this information was purchased by a potential employer, this supposed gambling-addicted psychologist may have trouble finding a job, since the field requires a very level head.

It seems that every piece of data that data brokers can collect on a person is worth something to someone. A company in Erie, Pennsylvania has a list of people with various addictions or in copious amounts of debt while a Connecticut based business advertises its lists of homosexual and bipolar adults (Kroft). These lists, for the right price, are publicly available at the click of a button. However, data collection companies have tried to keep the technical side of their business under wraps to dissuade a public uproar.

**Potential Benefits**

The price that you pay monthly for your internet stays with your ISP. It is the cost of service (e.g., infrastructure maintenance and additions). It is not distributed among the websites you visit. Yet, many of the websites across the web are not behind a paywall (i.e., a restriction on a website that requires a user to pay before accessing said website’s entire content). In fact, I do not believe that I have ever given a cent to Facebook, but it is still one of the world’s largest companies. However, this does not mean that most websites are free. Domains on the internet, and the businesses they represent, do not operate on altruism. They are in the game to make money. Advertisements are a large part of the way these companies prosper, and the more intrusive the ad, the more profit it generates. In the early days of internet advertisements, ads were randomly selected. Now, thanks to data brokers and their individual user records, these ads can be directed toward users who fit a target demographic (Criddle).

Directed ads help consumers contribute to the websites and brands they support. Many ads on the internet track what site you clicked on the ad from, giving an incentive for websites to showcase the ads they display in the best light possible (Criddle). YouTube, another popular website that most users do not pay for, plays ads either before or during a video as well as sometimes along the side of the video, often relating to the content of the video itself. Video creators get paid when a user interacts with an ad, not just when one is played. Personally, I am certainly more likely to click on an ad that I am interested in, which indirectly supports the content creator.

ISPs have the potential to make much more money if they begin to sell individual user data. This could bring the cost of internet down or could be invested in data communication technology. The United States, having a large population spread over thousands of miles, has had trouble keeping up with smaller countries in terms of internet speed per dollar. Across the US, whether in the tech hub of San Francisco or the farmlands of Kansas, for fifty dollars per month, the average internet speed is around twenty-five megabits per second. In Tokyo, for the same price, the internet speed can reach eight times that, with Seoul and Hong Kong being even faster (Yi). Increasing funding for data communication technologies as well as revamping our infrastructure (e.g., running fiber optic wires to more markets) would assist all customers by lowering prices and/or increasing speeds. Additionally, competition often arises when there is greater revenue in a market. As mentioned previously, many ISPs hold dominance over their service regions, acting almost as a monopoly. If creating an ISP became profitable without requiring a nationwide service region, new companies could break into the scene which would also help lower prices for internet users.

**Keeping your Data Private**

Small print in privacy policies are often what allow companies to legally collect and maintain data on mostly unsuspecting internet users. Luckily, we have a way to fight back. More and more websites are implementing HTTPS, an internet protocol that grants the user more security. When visiting sites which implement HTTPS (denoted by a lock icon in the URL bar on most browsers), the ISP can only see which websites are visited, not the data that is being communicated to that site via form fields. This protocol encrypts any data being transferred, therefore protecting the user from an ISP’s watchful eye (Brodkin).

Not all websites utilize this protocol yet, and even the ones that do still allow the ISP to see what pages a user visits. Virtual Private Networks (VPNs) block all of this from the ISP, so all that your ISP would see is that you are using a VPN. VPNs are rarely free and are often slower than normal internet browsing. Even when you pay for the ‘best’ VPN, the VPN provider can still track all your browsing, the same as an ISP would. The difference here is that while competing ISPs are hard to come by, VPN providers abound. Therefore, they are competing for a market that, right now, is not very large. This leads to a highly competitive marketplace where the consumer wins by having their demands met and their data kept safe (Brodkin).

The final, and arguably most secure option is The Onion Router (Tor), which, like an onion, consists of multiple layers of protection. Like a VPN, the ISP would only see that you are using Tor, but unlike a VPN, there is no one source that all your traffic is traveling through. Instead, every web interaction is bounced through “relays” that anonymize your web browsing (Brodkin).

**Conclusion**

Even if you were to implement every security step from now on or even stop using the internet all together, your web history is still up for grabs, as it most likely already been collected, perhaps just not yet sold.

Digital privacy is not only for those who have something to hide, it is for every user who has ever browsed the web. Digital brokers collect enough data from individual websites for them to serve us customized advertisements, and often store more data than we are comfortable with sharing. Allowing internet service providers to share in this data collection process oversteps ethical bounds and intrudes on our right to privacy online.

Work Cited

Bolluyt, Jess. "See How Much Money Your Social Networks Make Off Of You". *The Cheat Sheet*. N.p., 2017. Web. 10 Apr. 2017.

Brodkin, Jon. "How ISPs Can Sell Your Web History—And How To Stop Them". *Ars Technica*. N.p., 2017. Web. 10 Apr. 2017.

Cackley, Alicia Puente. *Information Resellers: Consumer Privacy Framework Needs To Reflect Changes In Technology And The Marketplace*. 1st ed. Washington, DC: United States Government Accountability Office, 2017. Web. 9 Apr. 2017.

Criddle, Linda. "How Do Free Websites Make Money?". *Webroot.com*. N.p., 2017. Web. 13 Apr. 2017.

"Data Broker Opt-Out List". *StopDataMining.me*. N.p., 2017. Web. 9 Apr. 2017.

Goel, Sharad, and Arvind Narayanan. "Why You Shouldn’t Be Comforted By Internet Providers’ Promises To Protect Your Privacy". *Slate Magazine*. N.p., 2017. Web. 10 Apr. 2017.

Klosowski, Thorin. "Congress Just Voted To Let Internet Providers Sell Your Web History". *Lifehacker.com*. N.p., 2017. Web. 9 Apr. 2017.

Kravets, David. "U.N. Report Declares Internet Access A Human Right". *Wired.com*. N.p., 2017. Web. 9 Apr. 2017.

Kroft, Steve. "The Data Brokers: Selling Your Personal Information". *CBSNews.com*. N.p., 2014. Web. 13 Apr. 2017.

"S.J.Res.34". *Congress.gov*. N.p., 2017. Web. 9 Apr. 2017.

Tarnoff, Ben. "Socialize The Internet". *Jacobinmag.com*. N.p., 2017. Web. 9 Apr. 2017.

"Xfinity Privacy Policy". *My.xfinity.com*. N.p., 2017. Web. 10 Apr. 2017.

Yi, Hannah. "This Is How Internet Speed And Price In The U.S. Compares To The Rest Of The World". *PBS NewsHour*. N.p., 2017. Web. 13 Apr. 2017.