

Joshua Berl

Comp 116: Computer Systems Security

Ming Chow

14 December 2016

## Terms and Conditions: What We Unknowingly Sign Away

### Abstract

Every time someone downloads a new application, creates an account on a web service, or uses practically anything online, they quickly dismiss the pop-up or check the box to claim “Yes, I agree to these terms and conditions.” Rarely do they take pause to read how Niantic is being given read and write privileges to their gmail account, (Pullen) or how Apple can turn logs of their iMessage use to law enforcement (Peterson). Are users ambivalent to their information being used however these companies please? Are the services they provide so good that users do not care? Or is the information presented in a way, in which consumers do not realize the implications of what they sign until they see headlines about it? Through a thorough analysis of the user agreements of Google, Facebook, and other information technology giants, and research through survey of what people think is a fair user agreement, this research will explore and attempt to resolve the confusion, misinformation, and presentation of information that surround user agreements. Users are socially engineered everyday into allowing applications and companies to use their information in an ever expanding litany of uses. The goal of this research is to explore and expose the use and misuse of user information by these entities, and explore other methods to protect users from blindly signing away their intellectual property and personal information.

“The cost of a thing is the amount of what I will call life which is required to be exchanged for it, immediately or in the long run.”

— Henry David Thoreau, Walden

When one uses an application, they must accept the terms and conditions of said application, yet these terms and conditions are rarely, if ever, read by the user. Sometimes these terms must be acknowledged, like checking a box in creating a Facebook profile, while other times the terms are implicitly accepted, with small messages, like Google’s, “By using our Services, you are agreeing to these terms. Please read them carefully” (google.com). Terms of Service; Didn’t Read, a user rights initiative that grades sites based on their terms of service, runs under the banner “‘I have read and agree to the Terms’ is the biggest lie on the web. We aim to fix that” (ToS;DR). This biggest lie on the web generally does not actively hurt users in the moment, but it does oftentimes ensure that sites have access and control of users’ personal information and data. Even so, this is not something that alarms users until they hear about a massive hack or those with access to the information using it in a way that surprises or offends them.

Some of this data collection and tracking has its positives for the user experience. Social Media sites can use big data for research and improved performance for the user, and using one’s profile and browsing information to target advertising to them provides users with relevant ads. These practices also make lots of money for the companies that provide these technologies, keeping them free of monetary cost to the user. While this exchange of information and privacy for service is not inherently underhanded or unethical, in practice the terms in which the

exchange exists are grossly unbalanced, favoring the rights and interests of the technologies and companies far more than those of the users. Many of these user agreements are hidden, obfuscated, and volatile, in that they are hard to find, difficult to read, and include a clause granting them the freedom to change the policies at any time (Doctorow).

Many are not concerned by the fact that sites can use browser cookies to decide which ads to display, but when it comes out that Uber employees have access to the ride information of all customers, people become more conscious and concerned about what of their information is collected and monitored (Evans). Users do not have the ability to pick and choose which parts of a user agreement they agree with and which they do not, and furthermore, the lexicon does not exist in how to determine whether or not a terms and conditions agreement is acceptable. The current landscape of these user agreements, intentionally designed to be hidden, ignored, and difficult to read, is one in which the user is socially engineered to give away as much information and lose as much privacy as these companies and technologies choose.

#### Why Is This Important?

Over one billion people use Facebook every day (Facebook). Google runs 100 billion search requests from over one billion users every month (Rey). This topic is relevant to a huge portion of people in the world, yet in an anonymous survey 94% of people claim that they do not read Terms and Conditions agreements before they accept and use an application. Of the same pool of subjects, 83% claimed that they should be able to control what information is being collected about them when they use free services like Google, Amazon, and Facebook and 70% claimed that it is not acceptable for these applications to profit off of their profile and personal information selling it to advertising services.

Many rely on an argument claiming, ‘I do not have anything to hide so I do not care if people can access my personal information,’ but this is a slippery slope. It is easy to justify the methods of these companies by acknowledging that they are in fact businesses that need to make money, and as users they must opt in to play by the companies’ rules, but when Twitter is the primary information channel between the President-Elect of the United States and the people, and Amazon is working to replace grocery stores with its own stores, users are more and more pressured to opt in. Again, these user agreements are written in a way that grossly favors the companies both legally and in terms of permissions, is unclear and intentionally difficult to read, and subject to change at any time. Many users were shocked to see that by default Apple’s iPhone tracks and logs all locations visited and the duration of each stay. This is just one of many examples of terms and default settings crossing the line that many users say is acceptable.

#### The Current Landscape of Privacy

Privacy is defined as the state or condition of being free from being observed or disturbed by other people, or freedom from unauthorized intrusion. This second half of the definition, the freedom from unauthorized intrusion, is where this topic gets murky, as users do authorize it. In clicking “I accept” users oftentimes waive their right to file a lawsuit, lose the rights to all original content that they post on a service, and agree that these rules can change anytime given their consent to the current set. While many services like Twitter and Instagram offer private accounts, in which the user decides who can follow and access the content posted, the default account is completely public. However, this is the current landscape of internet privacy, if one wants to be in control of their information and privacy, they must either opt out of the service entirely, not signing the terms and conditions agreement, or they must be knowledgeable enough

about the application or device itself to navigate the privacy settings to make them what the user wants.

Terms of Service; Didn't Read is an existing tool to help inform users about the terms of the sites they visit and use. It is a Chrome Extension and website that provides sites with a grade from Class A, in which the site provides "the best terms of service; they treat you fairly, respect your rights and will not abuse your data," to Class E, in which, "the terms of service raise very serious concerns" (ToS;DR). In this system Google earned a grade of C, the site citing, "Google keeps your searches and other identifiable user information for an undefined period of time... Google can use your content for all their existing and future services... This service tracks you on other websites... Google can share your personal information with other parties," as negatives, and "Google enables you to get your information out when a service is discontinued... Google posts notice of changes, with a 14-day ultimatum," as positives (ToS;DR). According to Terms of Service; Didn't Read, Google's terms are acceptable, but parts of it need the user's consideration. More importantly, this service looked through Google's Terms and Conditions and its Privacy Policy, which are long legal documents spread across several pages, and converted them into a digestible user friendly format, explaining what these terms mean to users. In this service, Google's C grade can be put into context next to Youtube's D, citing Youtube's continued storage of deleted content, as well as its ability to take down a user's content without notice. Github earned a B grade in that it does not take copyright licenses from users' content, and the very limited use of the personal information of its users. However, it is important to note that Github does make its money from advertising the way that Google and Youtube do.

In an anonymous survey, 86 participants were asked on a scale of 1 (strongly disagree) to 5 (strongly agree) how they felt about a number of statements about internet privacy and policy. The field of study or work did not seem to indicate any significant trends in the small sample size, but several of the questions provided nearly significantly one-sided results. 75% of participants disagree with the claim “everybody should be able to see everything I post on the internet.” 83% believe that they should have a say in what information about them is tracked and collected, and 84% of participants believe that they should have control of who has access to what they post. These figures indicate that control of personal information is important; however, when phrased in terms that include anonymity, 56% agreed to the more blanket statement, “I am alright with free services tracking my use habits and other information they have access to as long as I am anonymous.” Furthermore, when described in terms of increased performance, 57% of participants agreed to the statement “It is acceptable for services like Google Maps to track my location in order to predict traffic patterns and learn locations that I visit frequently in order to tailor options specifically to me and improve performance.” People are happy about customization and this sort of data collection when it benefits their user experience, and many do not mind it if it is anonymous. Participants care less about the fact that they are tracked and information is collected, but more that their names and information are tied to it. The participants do not see this form of data collection as inherently bad, and many even encourage it when it improves their experience using an application, but they would rather be one datum in a big set than a targeted and studied consumer that advertising agencies use as a tool and profile.

In the same study only 6% of participants claim that they read terms and conditions agreements before using new applications. This number is strikingly low given that upwards of

70% wanted complete autonomy over what information is collected and control over who can see it. Herein lies the dichotomy of the subject, people want control, but they also want to use new technologies, without having to read intentionally tedious documentation. Companies want to gain lots of users, which often requires the application to be free, but also need to make enough money to make the service worth providing, which often requires them to sell user information to advertisers. The current landscape is one defined by the terms of the companies and providers of the technologies. The pace at which these 'free by agreement' technologies have taken over has grossly outrun the ability of government or any large entity to regulate it. In the USA there is an FDA to protect consumers from unhealthy food and drugs, there is an SEC to protect consumers from predatory banks and financial institutions, but there is no regulatory institution to protect technology consumers from risky decisions. Regulation has failed to keep up with the explosion of technology in the last several years. The consequences of an online life void of privacy or autonomy of personal information do not appear the second one logs online, but this does not mean that it is inconsequential. If a lung tumor popped up the first time one smoked a cigarette, nobody would smoke.

#### Action and Application

First, a major overhaul is necessary in the delivery of terms and conditions to users. Currently they are designed to be off putting and difficult to read, full of legal jargon, and are oftentimes difficult to find and spread over several different pages. There needs to be a regulatory institution that provides a standard format that is easily accessible and understood by all users. Currently Terms of Service; Didn't Read provides a Google Chrome extension that

grades sites as a user visits them, where a click highlights what is good or bad for the user in the terms and conditions.

Another necessary change is to anonymize the collected information. Users do not mind being followed as anonymous data points, and the fact that users who visit Site A also visit Site B, is beneficial to advertisers, but people do not want their personal information stored for reasons that do not directly relate to the use of the application. Internally, companies must operate under the policy of minimum viable privileges, limiting what employees have access to to what is relevant to their work. Users should have the choice to opt in to having their information tracked and low privacy settings instead of having to opt out and the default settings set to public. As clear as some sites and applications try to make it to ramp up privacy, it would protect the average and casual users to make publicity an option instead of the norm.

On the other side of these issues, users must also be educated in how to read these terms; however, this can be quite difficult when companies like Apple have 25 page terms and conditions agreements that are updated frequently. This issue is not new, and it a system meant to keep users unaware and not in control of what they consent to in their click of the accept button. Given the current state of affairs, there is not much the average user can do to take action without giving up the service in question. Throughout the last several years, there have been many campaigns, like changing one's profile picture or posting that Facebook does not have permission to change its terms, but by using the product one is agreeing to all terms that the company defines. But if a regulatory agency could reformat the way this information is disseminated, perhaps the way most skip past terms and service agreements will change for the better, and people will know their rights.

Amazon Go (<https://www.amazon.com/b?node=16008589011>)

Doctorow, Cory. "The Curious Case of Internet Privacy." MIT Technology Review, 6 June 2012. Web. 11 Dec. 2016.

Evans, Will. "Uber Said It Protects You from Spying. Security Sources Say Otherwise." Reveal, 11 Dec. 2016. Web. 12 Dec. 2016.

Facebook (<http://newsroom.fb.com/company-info/>)

Google's Terms of Service Agreement (<https://www.google.com/intl/en/policies/terms/?fg=1>)

Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard UP, 2015. Print.

Peterson, Andrea. "Why Apple Can Be Forced to Turn Logs of Your iMessage Contacts over to Police." *Spokesman*, 30 Sept. 2016. Web. 13 Dec. 2016.

Pullen, John Patrick. "Pokemon Go Creator Says It's Not Reading Your Email." *Time*. Time, 12 July 2016. Web. 12 Dec. 2016.

Rey, Jason Del. "Google's Search Boss Talks Surviving and Thriving in an App World (Full Video)." *Recode*, 11 Oct. 2015. Web. 13 Dec. 2016.

ToS;DR Terms of Service; Didn't Read (<https://tosdr.org>)