# Agreeing to Terms and Conditions: An examination of privacy protection in a digital society

Senior Independent Project

Margaret Christovich

Spring 2019

# Abstract

The topic of this paper is the growing implications with digital privacy and the misuse of personal data. Privacy is something that as a user, I feel it is my responsibility to understand and be aware of. With communication and sharing becoming way easier than ever before, the need to balance privacy protection with the growth of technology is crucial. I was interested in researching digital privacy to better inform myself on my online actions as well as spread my knowledge with others to promote a more stable digital environment. I am also interested in pursuing computer science, so I think that a complete understanding of privacy would be beneficial for my future in a technology-related field.

My research was conducted mainly through journal articles and books. A few of my books were from the University of Maryland McKeldin library. My most useful source was Facebook's terms of service and privacy policy since they both provided excellent examples of how personal information is being used without the user's knowledge. I also interviewed Dr. Tracy Ann Kosa about her perspective on privacy since she has experience as a Senior Program Manager at Google and working with Microsoft. I found the interview very beneficial to my research, and gained a valuable perspective from Dr. Tracy Ann Kosa, a privacy expert.

In this paper, I will explore how unsuspecting users fall victim to the illusion of privacy that companies create which can lead to the misuse of personal data. First, I will define privacy and explore different types of information susceptible to being stolen. Then, I will examine numerous examples of major data breaches and privacy scandals. Finally, I will conclude by identifying the conflicts in balancing privacy in our market economy while also allowing growth in the technology-centered world.

The growth of technology has revolutionized means of communicating with others and provided incredible benefits in the growth of knowledge-and the progression of our species as a whole (Tedx Talks, 2017). Social platforms, such as Facebook, serve as a powerful tool for communicating with loved ones, building communities, and allowing everyone to have their voices heard (CNET, 2018). Facebook's mission is "to give people the power to build community and bring the world closer together" ("Terms of Service," 2018). The growth of these social platforms has also encouraged the sharing of personal information willingly on the Internet.

People share everything from names, emails, phone numbers, date of births, and addresses to what they ate for breakfast, relationship statuses, and political views (Gadekar & Pant, 2015, p. 273). As members of the digital community, it is necessary that users are rightfully informed how their data is being used. Many neglect their own privacy until they experience direct harm[1] of their own. It should not be socially acceptable for people to expect to suffer privacy harm while waiting for technologists to build safe systems (Computerphile, 2014).

[1] Harms may include having one's identity stolen, having personal information publicly exposed, or be a victim of credit card fraud

Because today's systems put privacy at risk, it is necessary to highlight the need for users to become educated on ways to protect their own privacy and demand that companies use their data fairly if they want to keep them as users.

In this paper, I will explore how unsuspecting users fall victim to the illusion of privacy that companies create which can lead to the misuse of personal data. First, I will define privacy and explore different types of information susceptible to being stolen. Then, I will examine numerous examples of major data breaches and privacy scandals. Finally, I will conclude by identifying the conflicts in balancing privacy in our market economy while also allowing growth in the technology-centered world.

**Define Privacy**

Privacy is the state of being free from being observed. Something can be considered private if one has control over who can access it. Consequently, the protection of privacy is the protection against unwanted access by other people. Limited access refers to a person's ability to avoid having other individuals and companies collect personal data. The term 'private' can be ascribed to "actions, situations, states of mind, places and objects" (Rössler, 2015, p. 9). Informational privacy[2] refers to monitoring others' access to personal information over technology (Daniela, 2015, p. 221). So, how much privacy is enough privacy, and when can a company be said to be invading our privacy?

Digital privacy does not make headline news until celebrity nudes are leaked or corporate emails are made public. Because our relationship with the Internet has reached an unprecedented level of connectedness, it is imperative that more emphasis is placed on privacy regulation as

[2] Data privacy

technology is evolving (Budge, Cooper, & Hoegg, 2016). The online world is becoming far more open to sharing information, but the legislation to ensure that private information remains private is not changing fast enough to keep up with that growth. A huge barrier in this legal shift is the lack of knowledge held by government officials on specific software before imposing privacy regulations (Andrews, 2013, p. 73).

**Implications of Digital Privacy**

Many approach the issue of privacy with the attitude that because they themselves are not guilty of anything and live a very open life already, there is no need to filter what information is shared about them. I have not committed any crimes, I am not incredibly wealthy, I am not a celebrity, so what can one really do with a chunk of my data?

The answer is power. Personal information can be used to exercise control, and, in the wrong hands, can be used to harm. If someone is trying to get an individual to do something they do not want to do, they may look at the victim's digital footprint[3] in order to create some sort of psychological leverage (Budge, Cooper, & Hoegg, 2016). In the Facebook-Cambridge Analytica scandal,[4] Cambridge Analytica had harvested the personal data from millions of Facebook profiles to build software that would predict and influence voters. By exploiting information such as interests, birthdays, location, online presence, and religion, messages were sent to users to promote Donald Trump's presidential campaign (Teague & Culnane, 2018).

Invasion of privacy can also hinder freedom of thought and speech. Always being monitored can result in restricted thought. Our behavior changes dramatically when we know we are being watched. We are more conformist and compliant. The decisions we make are often

[3] The information about a particular person that exists on the Internet as a result of their online activity

[4] Early 2018 data scandal, where Facebook profiles were used for political purposes. See Appendix A

byproducts of mandates of society (TED, 2014). Just as a celebrity must be aware of their actions since they always having a large audience observing and judging them, all individuals are more restricted knowing their actions and thoughts could be exposed to the public. People have the right to think, and explore new ideas, but the constant use of information is hindering one's ability to do so.

The inability to recover from privacy invasions also destroys second chances. With information freely exposed, one's ability to correct past mistakes is hindered. After a personal piece of information is leaked to the public, it is difficult to detach oneself from the humiliation of past moments. Because the Internet is an "integral piece of external memory" (Jones, 2016, p. 22), it prevents people from reinventing themselves. Digital memory does not forget the past.

## Information Susceptible to being Stolen

Everyone has a trail of data that can be collected and combined to construct a full profile of an individual. With just a name, an investigator can easily determine information such as addresses, family information, and political views. Data collected is not solely limited to information released on a computer, but can also be compiled with information gathered from phones, cars, credit cards, watches, and now even household appliances. With the complexity of devices growing, more personal information is being disclosed, processed, and discovered (Jones, 2016, p. 8).

*Who you are* is defined by personally identifiable information[5] which includes name, social security number, date of birth, email, and phone number. Companies also keep track of *what you do*. This may include sites visited, searches performed, purchases online, and articles

[5] See Appendix B (Krishnamurthy, 2009)

read. When *who you ar*e and *what you do* are easily identifiable, it raises concern for the protection of an individual's identity.

What information is collected and how that information is used on applications is all laid out in the Terms and Conditions and Privacy Policy which users agree to when creating an account or signing up to use an Internet network. Most users agree to the terms having not read the entirety of the agreement, if they read any part of it at all. The Facebook Terms and Conditions is over 87,000 words. A typical Terms and Service Agreement sets out 1) information you give the company access to and 2) how the information is used.

**Cases and Major Data Breaches**

In a federal class action lawsuit, *Robbins v. Lower Merion School District*, students attending Lower Merion High School were being monitored without rightful consent, and the school had to pay $610,000 to settle the lawsuit. The school issued Macbook Air laptops to the 2,306 students and loaded the computers with lanRev which included the now discontinued software "TheftTrack." Students were unaware that the school could monitor their communication and website history and access the laptops' webcams[6]. When the laptop's software was on, the webcam took a photo every 15 minutes using the built-in camera. School employees could adjust the frequency to as low as one photograph per minute. The laptop software then transmitted images to servers at the school where authorities reviewed them. Because LanRev discontinued the camera for all other uses, students assumed the camera was never active. The laptop was programmed to erase the sent file following delivery. In February 2010, Blake Robbins was accused by the school of inappropriate behavior at home. The evidence

[6] See Appendix C

was a photograph taken by the laptop's webcam in Robbins' home. On August 16, 2010, the school board finally banned the district from conducting webcam surveillance through students' laptops. *Robbins v. Lower Merion School District* demonstrates the need for privacy protection to be more strictly enforced (Hill, 2010).

Data brokers collect and analyze data on millions of people to then sell without the subjects' knowledge. Data is used to target advertise, offer credit risk assessment, and distribute direct marketing. Data brokers' need to obtain data is fueled by the promises of financial gain, fame, just because they can (Symantec employee, 2019). Personal information of individuals can be sold online to then be used to steal one's identity or commit fraud. There is a big surplus of stolen personally identifiable information, so the price to purchase is dropping on the dark web. The same goes for credit card numbers, which are now sold in bulk.

The number of global data breaches is increasing at an escalated pace. A data breach is the release of private information to an untrusted environment, whether intentional or unintentional. The types of data breaches include identity theft, account access, and financial access.

> "Now a new report by digital security specialists Gemalto reveals that 945 data breaches led to a staggering 4.5 billion data records being compromised worldwide in the first half of 2018, with the total number of breaches down year-on-year — but the number of records compromised up 133 percent as the severity of incident rises" (Targett, 2018).

The sources of data breaches range from malicious outsiders to accidental loss to malicious insiders. Many different industries can be impacted by a data breach including those in healthcare, finance, education, government, retail, and hospitality. Companies tend to spend more time responding to data breaches then they do implementing efforts to prevent them from happening in the first place (Bélanger & Crossler, 2011, p. 1018).

An unauthorized party had had access to the Starwood network database since 2014, yet it was only recently discovered in September 2018. Personal information of about 327 million people who made a reservation at a Starwood property may have been exposed. This breach included their names, phone numbers, mailing addresses, passport numbers, email addresses, dates of birth, genders and other personal information (Goldberg, 2018).

The Equifax data breach affected approximately 143 million users, which caused an estimated $439 million in loss for the company. This breach included names, Social Security numbers, dates of birth, addresses and driver's license numbers. 182,000 U.S. consumers' credit card numbers were also accessed (Goldberg, 2018).

**Balancing Privacy in our Market Economy**

Conflicts arise between balancing privacy rights of individuals in our market economy and the growing technology-centered world. New technology creates an illusion of privacy and control that increase the chance of victimization of its users. Consequently, the digital age is bringing tension between privacy protection and market efficiency. A market economy depends on a flow of information (Sarat, Douglas, & Umphrey, 2012, p. 9). Companies like Facebook, Instagram, and Twitter are designed for you to give away your information. It is a business and these businesses organize and sort every piece of information people disclose (Claypoole, 2014, p. 1). Social platforms are designed for you to spend as much time as possible using their application, and as such, apply psychological tricks to keep users on their site as long as possible and encourage them to keep coming back to their platform in the future (Tedx Talks, 2017). As an example, Facebook's Data Policy claims that they use an individual's data to create a more personalized experience:

> "To create personalized products that are unique and relevant to you, we use your connections, preferences, interests and activities based on the data we collect and learn from you and others (including any data with special protections you choose to provide); how you use and interact with our Products; and the people, places, or things you're connected to and interested in on and off our Products"(Facebook, 2018).

In order for Facebook to encourage users to remain interested in using their application, they have to collect and use an individual's data. If users were presented with ads that did not interest them, they would be less inclined to spend time on Facebook, in turn decreasing Facebook's customer usage, and directly affecting Facebook's profits.

Many applications give the impression that the user is rightfully informed of all that is going on with their information. Facebook implemented a privacy check-up[7] in response to the recent privacy scandals which allows users to review and adjust privacy settings. This simple 3-step check-up acts as a confidence booster to users on Facebook. However, little do they know that their released information is in danger of problems such as identity theft, data brokers, and misuse.

Privacy is, in many respects, an area of conflicting desires between the organization and the individual. It is important for companies to manage a careful balance in their approach to privacy policies. If companies go too far in taking data from consumers, they risk alienating their consumer base. However, if companies do not use enough of consumers' data, they leave themselves vulnerable to other companies filling the same niche and competing with them (Bélanger & Crossler, 2011, p. 1030). Many companies, such as Facebook, have discovered that

[7] See Appendix D

they need to take a more proactive role in protecting user privacy, as they have lost users who have experienced an invasion of privacy (CNET, 2018).

The question arises: is the individual responsible for protecting their own personal information or does that responsibility fall on the company collecting that information? Dr. Tracy Korsa, a senior project manager at Google and former Microsoft employee, believes “the average data subject can not possibly understand the complexities of network architecture, system design and data transfer to have any notion of how their information travels through electronic systems” (T. A. Kosa, personal communication, January 3, 2019). The complexity of the software is a huge barrier to the user understanding exactly what they are agreeing to when signing the terms and conditions.

**Future of Privacy and Introduction to Creative Project**

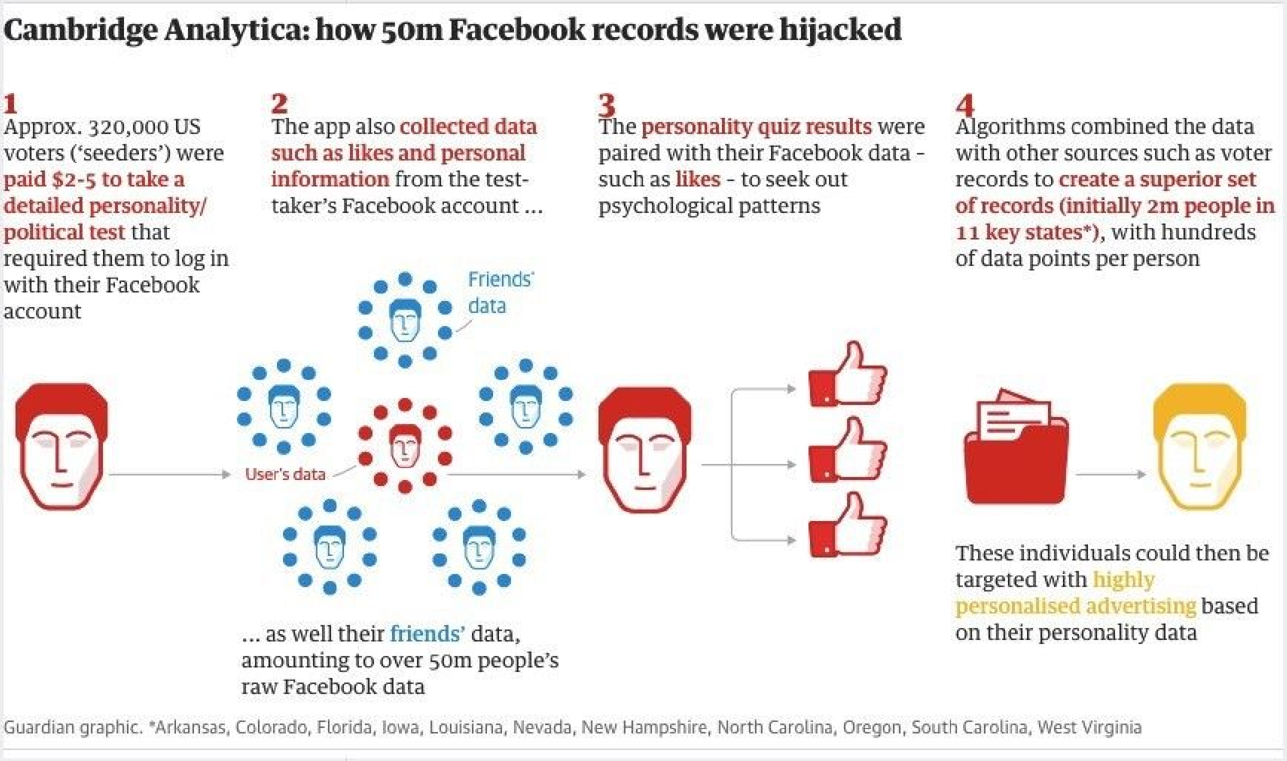
In our world of constant sharing and communication, it is difficult to find the right balance in terms of privacy. The issue begins with companies who gain the misplaced trust of users who then agree to their Terms and Conditions. Although major companies claim to safeguard the information the public releases to them, often times those assurances are proven false, as evident in the major data breaches occurring year-round. Dr. Tracy Korsa has observed a noticeable difference in companies’ attention to privacy issues between today and a decade ago (T. A. Kosa, personal communication, January 3, 2019).

In order to ensure people are better informed about future uses and protections of information they are giving away, the Terms and Conditions procedure needs to be adjusted. Currently, users check off the ‘I agree to the Terms and Conditions’ box as carelessly as they would sign their receipt at the grocery store. Efforts are currently being made to redesign Terms and Conditions, although change can be a slow process and it will take time before these efforts become standard (T. A. Kosa, personal communication, January 3, 2019). Efforts may include consolidating the length and complexity of the agreement to allow people to fully understand what they are agreeing to.

For my Senior Independent Project, I created a website to demonstrate the need for more concern for information sharing and to encourage users to actually read the terms to which they are agreeing to daily.[8] My website is public for anyone to see through the URL, and I will share my website with people to better inform them on how their privacy is at risk.

[8] See Appendix E

## Appendix A



**Cambridge Analytica: how 50m Facebook records were hijacked**

1
Approx. 320,000 US voters ('seeders') were **paid $2-5 to take a detailed personality/ political test** that required them to log in with their Facebook account

2
The app also **collected data such as likes and personal information** from the test-taker's Facebook account ...

3
The **personality quiz results** were paired with their Facebook data - such as **likes** - to seek out psychological patterns

4
Algorithms combined the data with other sources such as voter records to **create a superior set of records (initially 2m people in 11 key states*)**, with hundreds of data points per person

... as well their **friends'** data, amounting to over 50m people's raw Facebook data

These individuals could then be targeted with **highly personalised advertising** based on their personality data

Guardian graphic. *Arkansas, Colorado, Florida, Iowa, Louisiana, Nevada, New Hampshire, North Carolina, Oregon, South Carolina, West Virginia

Explanation of Cambridge Analytica Scandal
https://medium.com

## Appendix B

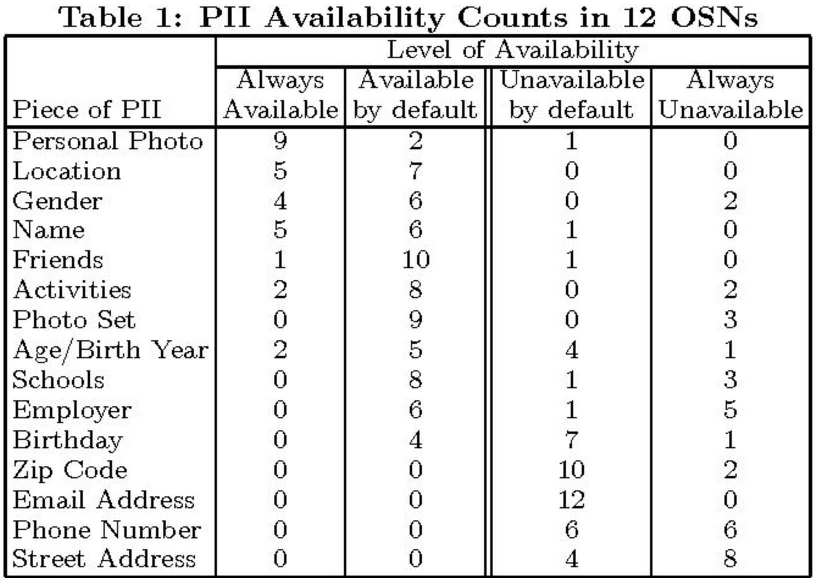
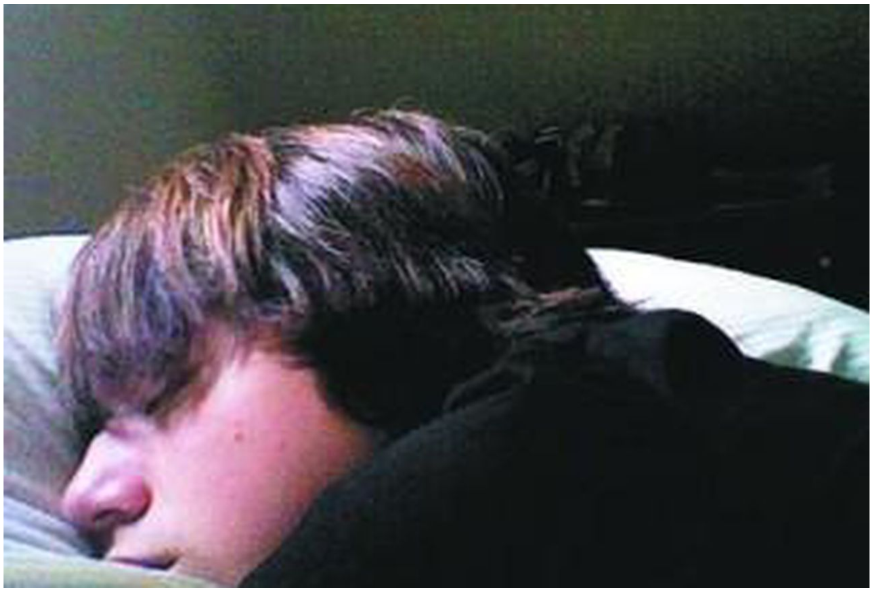


**Table 1: PII Availability Counts in 12 OSNs**

| | Level of Availability | | | |
|---|---|---|---|---|
| Piece of PII | Always Available | Available by default | Unavailable by default | Always Unavailable |
| Personal Photo | 9 | 2 | 1 | 0 |
| Location | 5 | 7 | 0 | 0 |
| Gender | 4 | 6 | 0 | 2 |
| Name | 5 | 6 | 1 | 0 |
| Friends | 1 | 10 | 1 | 0 |
| Activities | 2 | 8 | 0 | 2 |
| Photo Set | 0 | 9 | 0 | 3 |
| Age/Birth Year | 2 | 5 | 4 | 1 |
| Schools | 0 | 8 | 1 | 3 |
| Employer | 0 | 6 | 1 | 5 |
| Birthday | 0 | 4 | 7 | 1 |
| Zip Code | 0 | 0 | 10 | 2 |
| Email Address | 0 | 0 | 12 | 0 |
| Phone Number | 0 | 0 | 6 | 6 |
| Street Address | 0 | 0 | 4 | 8 |

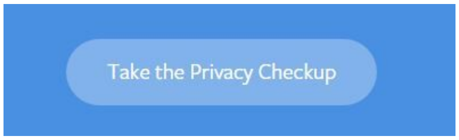
Prevalence of Personally Identifiable Information (PII) in 12 Online Social Networks (OSNs)
https://www.semanticscholar.org

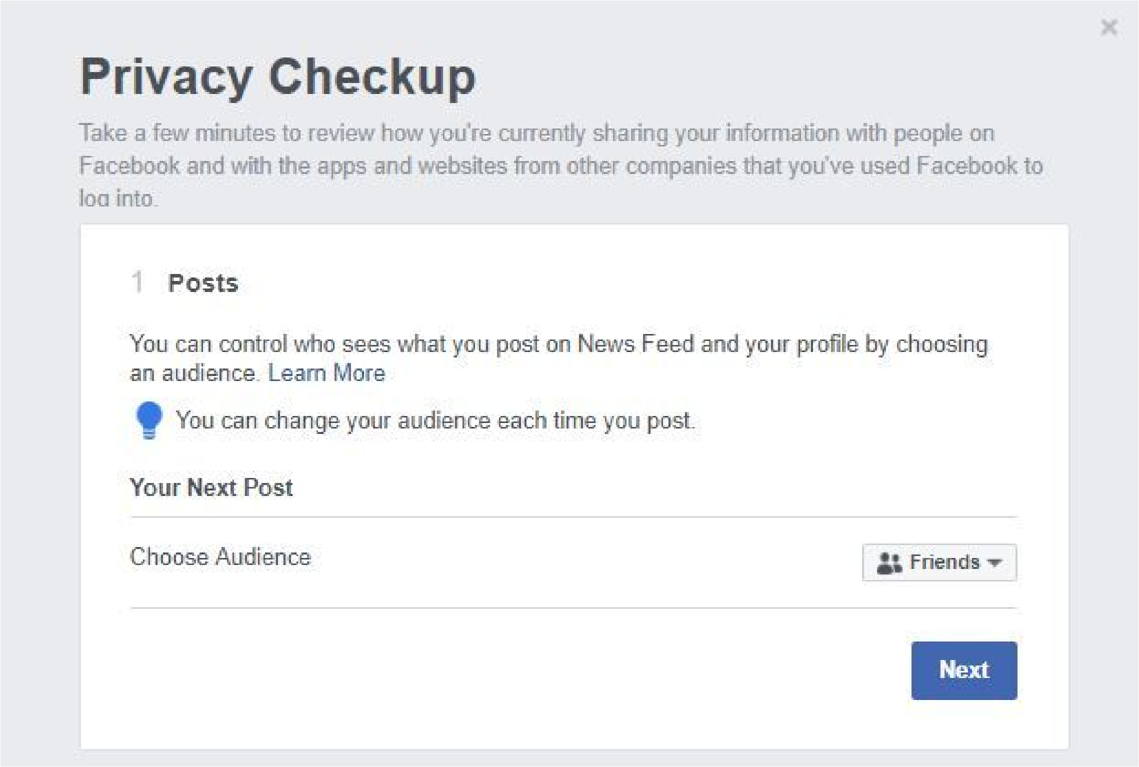
## Appendix C



Photograph taken off of Blake Robbins laptop camera
https://www.forbes.com

## Appendix D





Privacy Checkup

Take a few minutes to review how you're currently sharing your information with people on Facebook and with the apps and websites from other companies that you've used Facebook to log into.

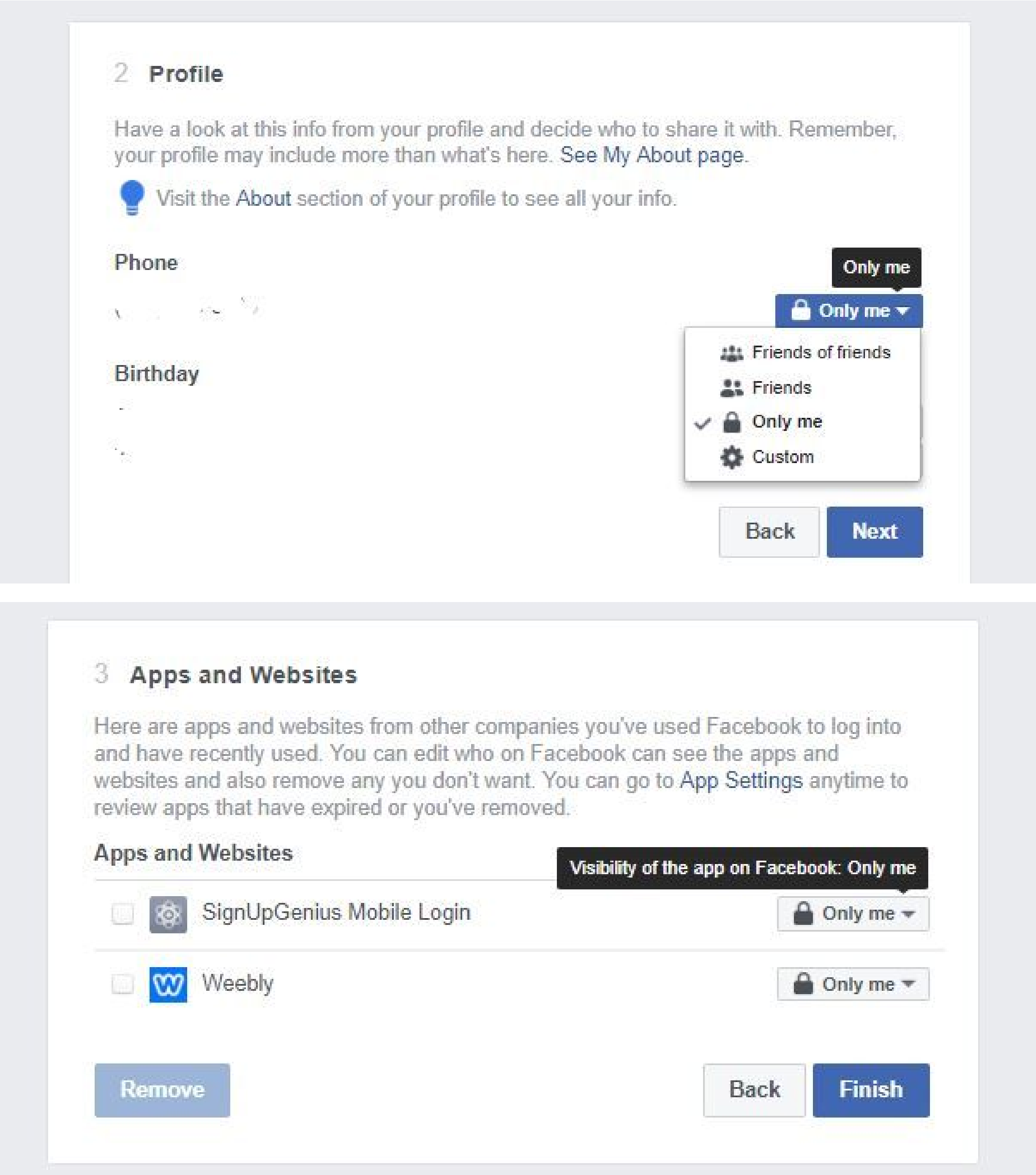
1 Posts

You can control who sees what you post on News Feed and your profile by choosing an audience. Learn More

You can change your audience each time you post.

Your Next Post

Choose Audience: Friends



2 Profile

Have a look at this info from your profile and decide who to share it with. Remember, your profile may include more than what's here. See My About page.

Visit the About section of your profile to see all your info.

Phone: Only me

Birthday

3 Apps and Websites

Here are apps and websites from other companies you've used Facebook to log into and have recently used. You can edit who on Facebook can see the apps and websites and also remove any you don't want. You can go to App Settings anytime to review apps that have expired or you've removed.

Apps and Websites

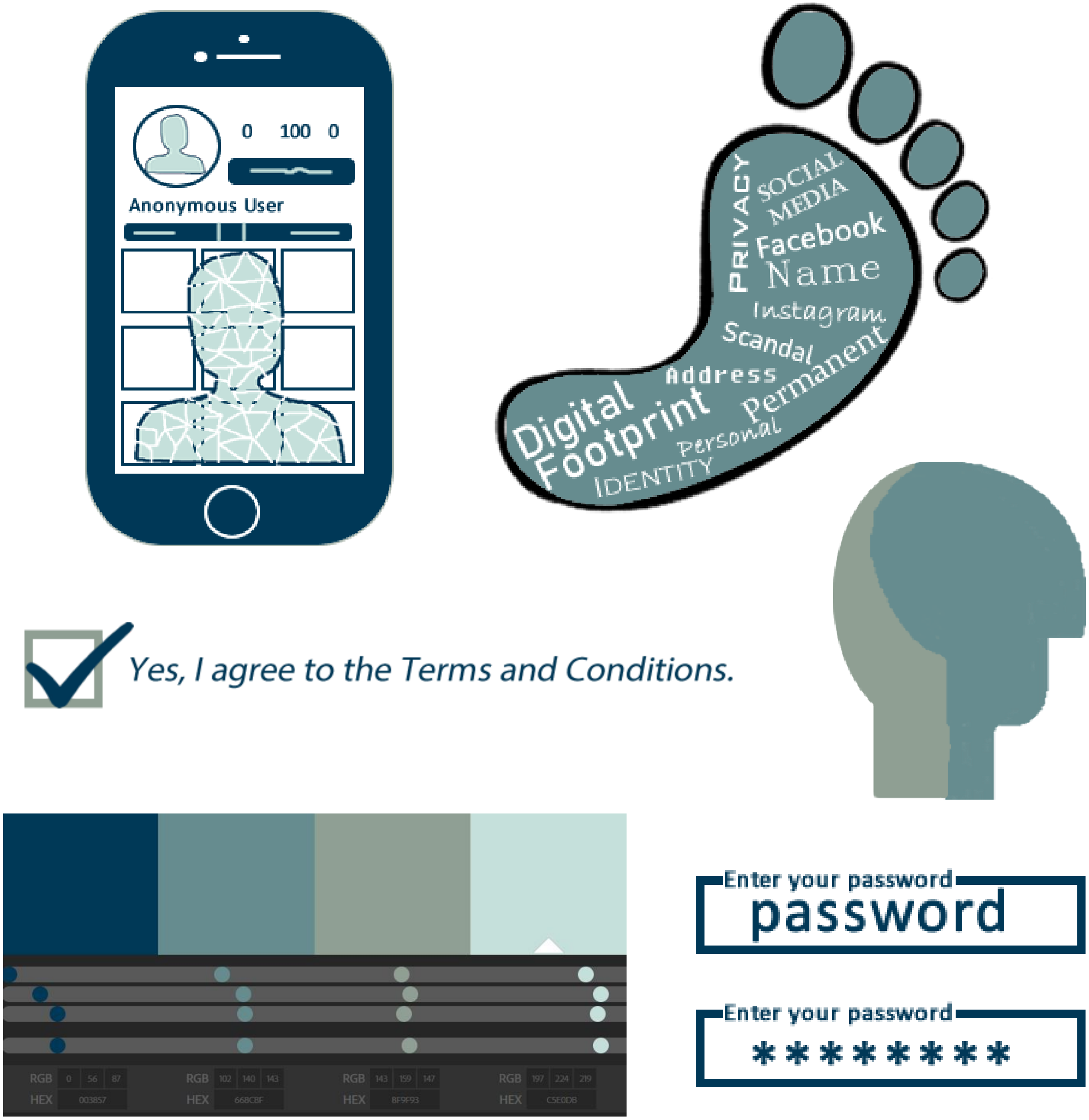
Visibility of the app on Facebook: Only me

□ SignUpGenius Mobile Login: Only me

□ Weebly: Only me

Facebook's 3-step privacy check-up
https://www.facebook.com

Appendix E



| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| RGB | 0 | 56 | 87 | RGB | 102 | 140 | 143 | RGB | 143 | 159 | 147 | RGB | 197 | 224 | 219 |
| HEX | 003857 | | | HEX | 668C8F | | | HEX | 8F9F93 | | | HEX | C5E0DB | | |

Original graphics and color scheme for my creative project website
http://sprigg.org/awt1819/margaret/sip/sip.html

# References

Andrews, L. B. (2013). *I Know who you are and I saw what you did: Social networks and the death of privacy*. New York [u.a.]Free Press.

Budge, C. (Producer), & Cooper, C., & Hoegg, M. (Directors). (2016). *The Power of Privacy* [Motion picture].

Belanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017-1041. https://doi.org/10.2307/41409971

Claypoole, T. F. (2014). Privacy and Social Media. *Business Law Today*, *1*(1), 1-4. https://doi.org/10599436

CNET. (2018, April 10). *Zuckerberg's Senate hearing highlights in 10 minutes* [Video file]. Retrieved from https://youtu.be/EgI_KAkSyCw

Computerphile. (2014, May 7). *Privacy in Social Media - Computerphile* [Video file]. Retrieved from https://youtu.be/Nqzo_VT7TQk

Daniela. (2015). Digital Communication and Privacy: Is Social Web Use gendered? *AAA: Arbeiten aus Anglistik und Amerikanistik*, *40*(1/2), 219-245. Retrieved from JSTOR database.

Facebook. (2018, April 19). Data Policy. Retrieved January 21, 2019, from Facebook website: https://www.facebook.com/full_data_use_policy

Gadekar, R., & Pant,, S. (2015). EXPLORING FACEBOOK USERS' PRIVACY KNOWLEDGE, ENACTMENT AND ATTITUDE: A STUDY ON INDIAN YOUTH.

*International Journal of Communication Research; Iasi*, *5*(4), 273-283. Retrieved from ProQuest Research Library Prep database. (Accession No. 1783990017)

Goldberg, M. (2018, November 30). 13 data breaches that stung US consumers. Retrieved January 28, 2019, from Bankrate website: https://www.bankrate.com/finance/banking/us-data-breaches-1.aspx#slide=1

Hill, K. (2010, October 11). Lower Merion School District and Blake Robbins Reach a Settlement in Spycamgate. *Forbes*.

Jones, M. L. (2016). *Ctrl + Z: The right to be forgotten*. New York, N.Y.: New York University Press.

Kosa, T. A. (2019, January 3). [E-mail interview by the author].

Krishnamurthy, B. (2009). On the leakage of personally identifiable information via online social networks. *WOSN*.

Sarat, A., Douglas, L., & Umphrey, M. M. (2012). *Imagining new legalities: Privacy and its possibilities in the 21st century*. Stanford, Calif.: Stanford University Press.

Symantec employee. (n.d.). Why your online privacy matters. Retrieved January 28, 2019, from Norton website: https://us.norton.com/internetsecurity-privacy-why-your-online-privacy-matters.html

Targett, E. (Ed.). (2018, October 9). 6 Months, 945 Data Breaches, 4.5 Billion Records. Retrieved December 15, 2018, from Computer Business Review website: https://www.cbronline.com/news/global-data-breaches-2018

Teague, V., & Culnane, C. (2018, March 28). Data Privacy and Power. Retrieved December 15, 2018, from Pursuit website: https://pursuit.unimelb.edu.au/articles/data-privacy-and-power

TED. (2014, October 10). *Glen Greenwald: Why privacy matters* [Video file]. Retrieved from https://youtu.be/pcSlowAhvUk

Tedx Talks. (2017, January 19). *Smartphones, Social Media & Modern Privacy | Alexi Bitsios | TEDxUniversityofKent* [Video file]. Retrieved from https://youtu.be/iyO-n5Fcu2Y

Terms of Service. (2018, April 19). Retrieved January 21, 2019, from Facebook website: https://www.facebook.com/terms.php