Surveillance Capitalism: Making Companies Accountable

Alice Lee
Tufts University
Comp116, Fall 2018

Abstract
Target collects customer data to predict future purchasing behavior. Equifax's modus operandi is selling aggregated user data. Facebook creates an advertisement profile for users based on their site activity. Understandably (in some cases), companies use personal information as a tool for targeted marketing, which drives consumer spending and higher profits. Although the data collected may seem basic and harmless, the combined information can have the power to not only predict and alter behavior, but also steal one's identity. With the number of breaches happening daily, the amount of data stored by these companies should be a concern. Sadly, it is not in the company's interest to protect user information. The paper will discuss some of the major breaches in the past few years, as well as changes implemented to prevent future breaches. It will also explore the European Union's latest data protection law and steps consumers can take to protect their personal information.

Introduction
Leaked user information is a common headline nowadays. Companies like Target, Equifax, Facebook, and Google were all involved in incidents where customer information was exposed. Consumer's names, email addresses, credit card numbers, and even Social Security numbers were among the types of information that was leaked or stolen (Table 1). The exploits came in different flavors: malware, out-of-date software, oversight on third-party permissions, and bugs. The leaks ranged from half a million user profiles from Google to 148 million people from Equifax due to their out-of-date software (Table 2). To give some perspective, Equifax's breach affected about 45% of the United States population. While it is important to understand how these attacks or leaks occurred, it is equally important to understand why these companies need to store sensitive information and what consumers can do to protect their personal information.

	Target	Equifax	Facebook	Google
Full Name	x		x	x
Phone Number	x	x	x	
Email Address	x	x	x	x
Credit Card Information	x	x		
Driver's License		x		
Social Security Number		x		

Date of Birth		x	x	
Physical Address		x		
User Location			x	
Raw User Profile			x	
Age				x
Occupation				x
Gender				x

Table 1. Target (McCoy, 2017), Equifax (Fleishman, 2018), Facebook (Graham-Harrison, 2018), Google (Statt, October 2018) and (Statt, December 2018) breaches or leaks and information exposed.

Company	When it happened	When it was announced	How many people it affected
Target	Between November 2013 and December 2013	December 2013	70 million
Equifax	Mid-May 2017 to July 2017	September 2017	148 million
Facebook	2013	March 2018	87 million
Google	Between 2015 and March 2018	October 2018	0.5 million
Google	Unknown	December 2018	52.5 million

Table 2. Target (McCoy, 2017), Equifax (Fleishman, 2018), Facebook (Graham-Harrison, 2018), Google (Statt, October 2018) and (Statt, December 2018) breaches or leaks. When it happened and how many people were affected.

Why do these companies need people's information?

On a basic level, Target, Equifax, Facebook, and Google can generate or increase their revenue through collecting and analyzing people's information.

Target, Facebook, and Google collect user information to better predict consumer behavior and create effective targeted advertisements, which results in higher sales and earnings. The more data these companies collect, the better and more accurate predictions they can make about a person's behavior. The information gives companies power to forecast and modify consumer decisions, which consequently generates revenue and market share (Zuboff, 2015). Shoshana Zuboff coined this behavior as surveillance capitalism, where companies collect large amounts of data in order to influence human behavior.

In 2002, Target created a pregnancy-prediction model. The company was interested in the forecast because the arrival of a baby means baby-related purchases. The company wanted consumers to create a habit of returning to Target for their baby product needs, as well as their other purchases. Each Target

customer has an internal Guest ID number, which links to every purchase the person has made at the store (Duhigg, 2012). Other information in the profile include the person's age, marital status, distance to store, location, estimated salary, and the kinds of credit cards owned (Duhigg, 2012). Target can also buy data about the person's ethnicity, job history, brand preference, where the person went to college, to name a few (Duhigg, 2012). By analyzing a combination of 25 products typically bought by expecting mothers, a Target analyst was able to predict whether a customer was expecting and their due date (Duhigg, 2012). Target would then send the customer baby-related coupons, which would later branch out to groceries, clothes, and other items on their shopping list. Between 2002 (when the pregnancy-prediction model started) and 2010, Target's revenue increased by more than 50% from $44 billion to $67 billion. Clearly, some marketing model was working.

Google and Facebook are, for the most part, free-to-use platforms. They generate their revenue through targeted advertisements. As of 2017, Google and Facebook control 63% of the U.S. digital advertising market (Blumenthal, 2018). In the same year, U.S. digital advertising spending reached $88 billion (IAB, 2018). The pair's marketing tactics are effective because it tailors the advertisements to fit the interest and needs of the consumer. Their targeted audience can be precise based on the data they have collected: user location history, education, hobbies, likes and dislikes, emails, and more. Effective and efficient advertisements lead to an increase in consumer spending, companies put more money into more targeted advertisement, and the cycle continues.

Equifax is a credit report agency and they give people credit scores based on their credit history. One's credit history includes number of credit accounts open, repayment history, amount of credit available or used, and outstanding debt collections (Irby, 2018). Credit report agencies also collect information through public records on bankruptcy, tax liens, foreclosures, and repossessions (Irby, 2018). In 2016, about 71% of Equifax's revenue came from aggregating consumers' information and selling it in bulk to other companies (Sweet, 2017). For example, banks like JP Morgan Chase want to target consumers who are thirty to forty years old with a credit score of 750 or above to sign up for new credit cards (Sweet, 2017). They can buy this information from Equifax and send out pre-approved credit card mailers to the targeted population (Sweet, 2017). In summary, Equifax generates revenue by selling consumer information and therefore will continue to collect people's information to sustain their business model. At this point, consumers cannot stop credit report agencies from collecting and selling their personal data.

It should be noted that some of the breaches were not directly involved with the large databases which stored customer information and behavior. However, the companies' negligence in these incidents prove that it is a ticking time bomb waiting to happen.

How are people affected?

Breaches or leaked information can affect people in two major ways: identity theft and influenced decisions.

When sensitive information is stolen, they are at risk of identity theft. People's date of birth, past addresses, and Social Security number are common information used to verify one's identity. With such

information in hand, thieves can use stolen credit card information to make unauthorized purchases, open new credit accounts with a stolen Social Security number, or use the Social Security number to apply for jobs under the victim's identity (Avoiding Identity Theft, 2017). Victims are left to deal with the aftermath, such as filing disputes to get their funds back, proving fraud activity, and rebuilding their credit score. Identity theft may not immediately happen after a breach, so consumers must be vigilant and keep a close eye on their credit reports or accounts. The impact of identity theft can take years to repair and can affect the victim's credit score, which determines if loans or lines of credit should be granted (Roberds, 2009).

Influenced decisions is subtle and the person may not know it is happening. In the Facebook and Cambridge Analytica data leak, it was reported that Cambridge Analytica used profiles to predict, target, and influence election votes. The organization created an algorithm which identified possible swing voters (Graham-Harrison and Cadwalladr, 2018). The campaign could then design messages that would resonate with the undecided voters and sway their votes (Graham-Harrison and Cadwalladr, 2018). The people who were influenced may never realize the impact of these subtle messages.

Similarly, brands use data to predict what and when a customer needs a product. When the company estimates that the customer is ready for the product, ads or discounts will appear on the customer's feed and influence them to purchase the product. Unless the consumer is aware of these tactics behind the scenes, they will never realize how or when they were influenced.

What has been done since the breaches?

Target paid a combined $68.5 million to fines and compensations (Thomson, 2017). Shockingly, Equifax paid no fines (Whittaker, September 2018). A report from the House Oversight Committee stated the breach was "entirely preventable", had Equifax followed basic security measures (Whittaker, December 2018). Although Facebook was also not legally fined, their stock dropped 20% after the privacy scandal (Statt, 2018).

Target committed $100 million to updating technology, such as secure payment machines with a physical chip on the cards (Clark, 2015). The company joined two cybersecurity threat-sharing initiatives, which allows companies to share cyber threat information and government cyber-analysts to investigate the threats (Clark, 2015). They updated their network infrastructure, implemented two-factor authentication, limited vendor access to networks, and reduced privileges on contractor accounts (Gagliordi, 2015). In addition, Target spent $5 million to educate consumers on cyber security risks (Manworren, 2016).

After the breach, Equifax budgeted an additional $200 million on security and technology, but did not provide details on what kind of technology (Fleishman, 2018).

Facebook set goals for changes that include making it easier for users to see app settings, tightening data access from apps, removing inactive apps, making it harder to find people, stop some targeted advertising, making advertiser information more transparent, and further researching the impact of social media on elections (Ivanova, 2018).

As for Google, they completely shut down the Google+ platform (Statt, 2018).

These strategies might be working because no new breaches were reported, but it is hard to tell.

Case Study: European Union's General Data Protection Regulation

In May 2018, the European Union passed the General Data Protection Regulation (GDPR) which allowed users to have more control over their data. Users who live in the EU must grant companies permission to collect, save, and use their information. The types of data covered include any kind of personal information, such as posts on social media, mailing addresses, IP addresses, and GPS locations (Shahani, 2018). Companies must explicitly request and ask consumers if they can save or use their information. For previously collected information, consumers can request for their data to be deleted. Companies can choose to comply with the regulation or pay a fine. Any company which saves consumer information is affected (Hern, 2018). GDPR not only gives consumers control over their personal information, it also holds companies accountable with people's data, especially when the information is breached or leaked. Because of the penalty, companies make it a higher priority to protect and respect user's data. GDPR is a step towards better data protection and gives consumers the power to control their personal information.

What can consumers do?

There are a couple of things consumers can influence change through legislation and spreading awareness.

Current regulations in the United States are insufficient to encourage companies to secure customer's data. The fines are small and do not put the company at risk of bankruptcy or financial peril, companies would rather pay a fine (or no repercussions in Equifax's case) than to take the effort to secure their data (Manworren, 2016). It's not to say companies should go bankrupt over a mistake, but there should be a penalty that will make companies careful and make an effort to avoid preventable mistakes. These regulations can be changed or introduced by electing government officials who will fight for consumer rights and data protection.

Other regulations can include asking consumers to give companies permission to store, use, and distribute their data. Companies should face a penalty when they go against the consumer's wish, similar to the European Union's GDPR. Companies should also be required by law to disclose within a certain number of days if a breach happened.

In January 2018, two U.S. senators introduced the Data Breach Prevention and Compensation Act of 2018. The Senate Bill was triggered by Equifax's breach in 2017. The bill requires companies to undergo cybersecurity inspections, compensations for victims, and penalties, which can result from not reporting the breaches in a timely manner. If it were passed before the breach, it would cost Equifax $1.5 billion in fines (Miller, 2018). This penalty would have accounted for a little under 50% of Equifax's revenue of

$3.51 billion in 2016, a year before the incident (Sweet, 2017). The penalty is large enough to make an impact and not completely cripple the company. It sends a clear message that data security is a serious issue and should be a priority.

In addition to supporting and electing government officials (or even becoming one), consumers can let their monetary spending do the talking. By supporting companies who put an effort and care about consumer data protection, other companies will follow because they don't want to lose business. Companies will hopefully take initiative and make consumer data protection a priority. By choosing companies based on their commitment on data security, customers are sending a message that the safety of their data matters. When money is on the line, companies will listen and take action.

Lastly, consumers should educate themselves and others on cybersecurity risks, as well as how companies are using their personal information. They need to be aware of the latest news, breaches, or techniques used to steal and manipulate people's information. Consumers need to be mindful of the data they're sharing with companies and how this data will be used. They need to analyze their decisions, question how and why they were made. Without the proper laws and regulations, consumers cannot stop companies from collecting, using, and selling their personal data (Valentino DeVries, 2018). People need to stay up-to-date on the latest threats and make the right judgement to protect their personal information.

Conclusion

Databases filled with consumer information are growing by the second and the more data it contains, the more valuable it is. With the breaches and data leaks happening constantly, it's a matter of time before an attacker gets their hands on these large databases. Companies need to work harder to protect this data before it's too late. Regulation and penalties need to be imposed to motivate companies to secure personal information. Consumers need to take a proactive role by participating in activities which support data protection. They can also take measures to protect their personal information, such as monitoring their credit activity and being mindful of the information they share with companies. At the end of the day, consumers are the only protectors of their personal data.

Bibliography

"Avoiding Identity Theft." *Consumer.gov*, 5 June 2017, www.consumer.gov/articles/1015-avoiding-identity-theft.

Blumenthal, Paul. "Facebook And Google's Surveillance Capitalism Model Is In Trouble." *The Huffington Post*, The Huffington Post, 29 Jan. 2018, www.huffingtonpost.com/entry/facebook-google-privacy-antitrust_us_5a625023e4b0dc592a088f6c.

Clark, Meagan. "Timeline of Target's Data Breach And Aftermath: How Cybertheft Snowballed For The Giant Retailer." *International Business Times*, 6 Dec. 2015, www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056.

"Digital Ad Spend Reaches an All-Time High of $88 Billion in 2017, With Mobile Upswing Unabated, Accounting for 57% of Revenue." *IAB - Empowering the Marketing and Media Industries to Thrive in the Digital Economy*, 10 May 2018, www.iab.com/news/digital-ad-spend-reaches-all-time-high-88-billion-2017-mobile-upswing-unabated-accounting-57-revenue/.

Duhigg, Charles. "How Companies Learn Your Secrets." *The New York Times*, 16 Feb. 2012, www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

Elizabeth, Warren, and Mark Warner. "Data Breach Prevention and Compensation Act of 2018." *Congress.gov*, 12 July 2018, www.congress.gov/bill/115th-congress/senate-bill/2289/text.

Fleishman, Glenn. "Equifax Data Breach, One Year Later: Obvious Errors and No Real Changes, New Report Says." *Fortune*, 8 Sept. 2018, fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/.

Gagliordi, Natalie. "The Target Breach, Two Years Later." *ZDNet*, 4 Dec. 2015, www.zdnet.com/article/the-target-breach-two-years-later/.

Graham-Harrison, Emma, and Carole Cadwalladr. "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." *The Guardian*, 17 Mar. 2018, www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Hern, Alex. "What Is GDPR and How Will It Affect You?" *The Guardian*, 21 May 2018, www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you.

Irby, LaToya. “Every Consumer Should Know These 8 Things About Credit Bureaus.” *The Balance Small Business*, The Balance, 20 Oct. 2018, www.thebalance.com/credit-bureau-facts-960693.

Ivanova, Irina. “8 Promises from Facebook after Cambridge Analytica.” *CBS News*, 10 Apr. 2018, www.cbsnews.com/news/facebooks-promises-for-protecting-your-information-after-data-breach-scandal/.

Manworren, Nathan, et al. “Why You Should Care about the Target Data Breach.” *Business Horizons*, vol. 59, no. 3, May 2016, pp. 257–266., doi:10.1016/j.bushor.2016.01.002.

McCoy, Kevin. “Target to Pay $18.5M for 2013 Data Breach That Affected 41 Million Consumers.” *USA Today*, 23 May 2017, www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/.

Miller, Hayley. “Elizabeth Warren Wants Companies That Expose Your Data To Hackers To Pay Up.” *The Huffington Post*, 10 Jan. 2018, www.huffingtonpost.com/entry/elizabeth-warren-equifax-bill_us_5a561c07e4b03417e873e3c9.

Newman, Lily Hay. “Equifax's Security Overhaul, a Year After Its Epic Breach.” *Wired*, 25 July 2018, www.wired.com/story/equifax-security-overhaul-year-after-breach/.

Roberds, William, and Stacey L. Schreft. “Data Breaches and Identity Theft.” *Journal of Monetary Economics*, vol. 56, no. 7, 2009, pp. 918–929., doi:10.1016/j.jmoneco.2009.09.003.

Shahani, Aarti. “3 Things You Should Know About Europe's Sweeping New Data Privacy Law.” *NPR*, 24 May 2018, www.npr.org/sections/alltechconsidered/2018/05/24/613983268/a-cheat-sheet-on-europe-s-sweeping-privacy-law.

Statt, Nick. “Google Hid Major Google Security Flaw That Exposed Users' Personal Information.” *The Verge*, 8 Oct. 2018, www.theverge.com/2018/10/8/17951914/google-plus-data-breach-exposed-user-profile-information-privacy-not-disclosed.

Statt, Nick. “Facebook Growth Slows in Aftermath of Privacy Scandals.” *The Verge*, 25 July 2018, www.theverge.com/2018/7/25/17614518/facebook-q2-2018-earnings-cambridge-analytica-scandal-growth-stalling.

Statt, Nick, and Russell Brandom. “Google Will Shut down Google Four Months Early after Second Data Leak.” *The Verge*, 10 Dec. 2018, www.theverge.com/2018/12/10/18134541/google-plus-privacy-api-data-leak-developers.

Sweet, Ken. “Equifax Makes Money by Knowing a Lot about You.” *USA Today*, 6 Oct. 2017, www.usatoday.com/story/money/personalfinance/2017/10/06/equifax-makes-money-knowing-lot-you/738824001/.

Thomson, Iain. “Target Inks $18.5m Deal with US States to Settle 2013 Data Breach.” *The Register*, 24 May 2017, www.theregister.co.uk/2017/05/23/target_185m_deal_2013_data_breach/.

Valentino DeVries, Jennifer, et al. “Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret.” *The New York Times*, 10 Dec. 2018, www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

Whittaker, Zack. “Equifax Breach Was 'Entirely Preventable' Had It Used Basic Security Measures, Says House Report.” *TechCrunch*, 10 Dec. 2018, techcrunch.com/2018/12/10/equifax-breach-preventable-house-oversight-report/.

Whittaker, Zack. “A Year Later, Equifax Lost Your Data but Faced Little Fallout.” *TechCrunch*, 8 Sept. 2018, techcrunch.com/2018/09/08/equifax-one-year-later-unscathed/.

Zuboff, Shoshana. “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization.” *Journal of Information Technology*, vol. 30, no. 1, 2015, pp. 75–89., doi:10.1057/jit.2015.5.