Testimony and Statement for the Record of

Bruce Schneier
Fellow and Lecturer, Belfer Center for Science and International Affairs, Harvard Kennedy School
Fellow, Berkman Center for Internet and Society at Harvard Law School

Hearing on "Securing Consumers' Credit Data in the Age of Digital Commerce"

Before the

Subcommittee on Digital Commerce and Consumer Protection
Committee on Energy and Commerce
United States House of Representatives

1 November 2017
2125 Rayburn House Office Building
Washington, DC 20515

Mister Chairman and Members of the Committee, thank you for the opportunity to testify today concerning the security of credit data. My name is Bruce Schneier, and I am a security technologist. For over 30 years I have studied the technologies of security and privacy. I have authored 13 books on these subjects, including *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your* World (Norton, 2015). My popular newsletter Crypto-Gram and my blog *Schneier on* Security are read by over 250,000 people.

Additionally, I am a Fellow and Lecturer at the Harvard Kennedy School of Government—where I teach Internet security policy—and a Fellow at the Berkman-Klein Center for Internet and Society at Harvard Law School. I am a board member of the Electronic Frontier Foundation, AccessNow, and the Tor Project; and an advisory board member of Electronic Privacy Information Center and VerifiedVoting.org. I am also a special advisor to IBM Security and the Chief Technology Officer of IBM Resilient.

I am here representing none of those organizations, and speak only for myself based on my own expertise and experience.

I have eleven main points:

1. The Equifax breach was a serious security breach that puts millions of Americans at risk.

Equifax reported[1] that 145.5 million US customers, about 44% of the population, were impacted by the breach. (That's the original 143 million plus the additional 2.5 million disclosed a month later.[2]) The attackers got access to full names, Social Security numbers, birth dates, addresses, and driver's license numbers.

This is exactly the sort of information criminals can use to impersonate victims to banks, credit card companies, insurance companies, cell phone companies and other businesses vulnerable to fraud. As a result, all 143 million US victims are at greater risk of identity theft, and will remain at risk for years to come. And those who suffer identify theft will have problems for months, if not years, as they work to clean up their name and credit rating.

2. Equifax was solely at fault.

This was not a sophisticated attack. The security breach was a result of a vulnerability in the software for their websites: a program called Apache Struts. The particular vulnerability was fixed by Apache in a security patch that was made available on March 6, 2017.[3] This was not a minor vulnerability; the computer press at the time called it "critical."[4] Within days, it was being used by attackers to break into web servers. Equifax was notified by Apache, US CERT, and the Department of Homeland Security about the vulnerability, and was provided instructions to make the fix.[5]

---

[1] https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

[2] https://www.nytimes.com/2017/10/02/business/equifax-breach.html

[3] https://cwiki.apache.org/confluence/display/WW/S2-045

[4] https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/

[5] https://arstechnica.com/information-technology/2017/10/a-series-of-delays-and-major-errors-led-to-massive-equifax-breach/

Two months later, Equifax had still failed to patch its systems. It eventually got around to it on July 29.[6] The attackers used the vulnerability to access the company's databases and steal consumer information on May 13, over two months after Equifax should have patched the vulnerability.[7]

The company's incident response after the breach was similarly damaging. It waited nearly six weeks before informing victims that their personal information had been stolen and they were at increased risk of identity theft. Equifax opened a website to help aid customers, but the poor security around that—the site was at a domain separate from the Equifax domain—invited fraudulent imitators and even more damage to victims. At one point, the official Equifax communications even directed people to that fraudulent site.[8]

This is not the first time Equifax failed to take computer security seriously. It confessed to another data leak in January 2017. In May 2016, one of its websites was hacked, resulting in 430,000 people having their personal information stolen. Also in 2016, a security researcher found and reported a basic security vulnerability in its main website. And in 2014, the company reported yet another security breach of consumer information. There are more.[9]

3. There are thousands of data brokers with similarly intimate information, similarly at risk.

Equifax is more than a credit reporting agency. It's a data broker.[10] It collects information about all of us, analyzes it all, and then sells those insights. It might be one of the biggest, but there are 2,500 to 4,000 other data brokers that are collecting, storing, and selling information about us—almost all of them companies you've never heard of and have no business relationship with.

The breadth and depth of information that data brokers have is astonishing. Data brokers collect and store billions of data elements covering nearly every US consumer. Just one of the data

---

[6] https://arstechnica.com/tech-policy/2017/09/equifax-cio-cso-retire-in-wake-of-huge-security-breach/

[7] https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/

https://arstechnica.com/information-technology/2017/10/a-series-of-delays-and-major-errors-led-to-massive-equifax-breach/

[8] https://www.nytimes.com/2017/09/20/business/equifax-fake-website.html

[9] https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/

[10] https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

brokers studied holds information on more than 1.4 billion consumer transactions and 700 billion data elements, and another adds more than 3 billion new data points to its database each month.[11]

These brokers collect demographic information: names, addresses, telephone numbers, e-mail addresses, gender, age, marital status, presence and ages of children in household, education level, profession, income level, political affiliation, cars driven, and information about homes and other property. They collect lists of things we've purchased, when we've purchased them, and how we paid for them. They keep track of deaths, divorces, and diseases in our families. They collect everything about what we do on the Internet.

4. These data brokers deliberately hide their actions, and make it difficult for consumers to learn about or control their data.

If there were a dozen people who stood behind us and took notes of everything we purchased, read, searched for, or said, we would be alarmed at the privacy invasion. But because these companies operate in secret, inside our browsers and financial transactions, we don't see them and we don't know they're there.

Regarding Equifax, few consumers have any idea what the company knows about them, who they sell personal data to or why. If anyone knows about them at all, it's about their business as a credit bureau, not their business as a data broker.[12] Their website lists 57 different offerings for business: products for industries like automotive, education, health care, insurance, and restaurants.[13]

In general, options to "opt-out" don't work with data brokers. It's a confusing process, and doesn't result in your data being deleted. Data brokers will still collect data about consumers who opt out. It will still be in those companies' databases, and will still be vulnerable. It just don't be included individually when they sell data to their customers.

5. The existing regulatory structure is inadequate.

---

[11] https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more

[12] https://www.forbes.com/sites/forrester/2017/09/08/equifax-does-more-than-credit-scores/#1e73610019d8

[13] http://www.equifax.com/business/

Right now, there is no way for consumers to protect themselves. Their data has been harvested and analyzed by these companies without their knowledge or consent. They cannot improve the security of their personal data, and have no control over how vulnerable it is. They only learn about data breaches when the companies announce them—which can be months after the breaches occur—and at that point the onus is on them to obtain credit monitoring services or credit freezes. And even those only protect consumers from some of the harms, and only those suffered after Equifax admitted to the breach.

Right now, the press is reporting "dozens" of lawsuits against Equifax from shareholders, consumers, and banks.[14] Massachusetts has sued Equifax for violating state consumer protection and privacy laws.[15] Other states may follow suit.[16]

If any of these plaintiffs win in the court, it will be a rare victory for victims of privacy breaches against the companies that have our personal information. Current law is too narrowly focused on people who have suffered financial losses directly traceable to a specific breach. Proving this is difficult. If you are the victim of identity theft in the next month, is it because of Equifax or does the blame belong to another of the thousands of companies who have your personal data? As long as one can't prove it one way or the other, data brokers remain blameless and liability free.

Additionally, much of this market in our personal data falls outside the protections of the Fair Credit Reporting Act. And in order for the Federal Trade Commission to levy a fine against Equifax, it needs to have a consent order and then a subsequent violation. Any fines will be limited to credit information, which is a small portion of the enormous amount of information these companies know about us. In reality, this is not an effective enforcement regime.

Although the FTC is investigating Equifax, it is unclear if it has a viable case.[17]

6. The market cannot fix this because we are not the customers of data brokers.

---

[14] https://www.washingtonpost.com/news/business/wp/2017/09/22/after-the-breach-equifax-now-faces-the-lawsuits/?utm_term=.1fd423f6b3aa

[15] http://money.cnn.com/2017/09/12/news/equifax-lawsuit-massachusetts/index.html

[16] http://money.cnn.com/2017/09/19/technology/equifax-legal-issues/index.html

[17] https://www.washingtonpost.com/news/the-switch/wp/2017/09/14/the-ftc-confirms-its-investigating-the-equifax-breach-adding-to-a-chorus-of-official-criticism/

The customers of these companies are people and organizations who want to buy information: banks looking to lend you money, landlords deciding whether to rent you an apartment, employers deciding whether to hire you, companies trying to figure out whether you'd be a profitable customer—everyone who wants to sell you something, even governments.

Markets work because buyers choose from a choice of sellers, and sellers compete for buyers. None of us are Equifax's customers. None of us are the customers of any of these data brokers. We can't refuse to do business with the companies. We can't remove our data from their databases. With few limited exceptions, we can't even see what data these companies have about us or correct any mistakes.

We are the product that these companies sell to their customers: those who want to use our personal information to understand us, categorize us, make decisions about us, and persuade us.

Worse, the financial markets reward bad security. Given the choice between increasing their cybersecurity budget by 5%, or saving that money and taking the chance, a rational CEO chooses to save the money. Wall Street rewards those whose balance sheets look good, not those who are secure. And if senior management gets unlucky and the a public breach happens, they end up okay. Equifax's CEO didn't get his $5.2 million severance pay, but he did keep his $18.4 million pension. Any company that spends more on security than absolutely necessary is immediately penalized by shareholders when its profits decrease.

Even the negative PR that Equifax is currently suffering will fade. Unless we expect data brokers to put public interest ahead of profits, the security of this industry will never improve without government regulation.

7. We need effective regulation of data brokers.

In 2014, the Federal Trade Commission recommended that Congress require data brokers be more transparent and give consumers more control over their personal information.[18] That report contains good suggestions on how to regulate this industry.

First, Congress should help plaintiffs in data breach cases by authorizing and funding empirical research on the harm individuals receive from these breaches.

---

[18] https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more

Specifically, Congress should move forward legislative proposals that establish a nationwide "credit freeze"—which is better described as changing the default for disclosure from opt-out to opt-in—and free lifetime credit monitoring services. By this I do not mean giving customers free credit-freeze options, a proposed by Senators Warren and Schatz[19], but that the default should be a credit freeze.

The credit card industry routinely notifies consumers when there are suspicious charges. It is obvious that credit reporting agencies should have a similar obligation to notify consumers when there is suspicious activity concerning their credit report.

On the technology side, more could be done to limit the amount of personal data companies are allowed to collect. Increasingly, privacy safeguards impose "data minimization" requirements to ensure that only the data that is actually needed is collected. On the other hand, Congress should not create a new national identifier to replace the Social Security Numbers.[20] That would make the system of identification even more brittle. Better is to reduce dependence on systems of identification and to create contextual identification where necessary.

Finally, Congress needs to give the Federal Trade Commission the authority to set minimum security standards for data brokers and to give consumers more control over their personal information. This is essential as long as consumers are these companies' products and not their customers.

8. Resist complaints from the industry that this is "too hard."

The credit bureaus and data brokers, and their lobbyists and trade-association representatives, will claim that many of these measures are too hard. They're not telling you the truth.

Take one example: credit freezes. This is an effective security measure that protects consumers, but the process of getting one and of temporarily unfreezing credit is made deliberately onerous by the credit bureaus. Why isn't there a smartphone app that alerts me when someone wants to access my credit rating, and lets me freeze and unfreeze my credit at the touch of the screen? Too hard? Today, you can have an app on your phone that does something similar if you try to log into a computer network, or if someone tries to use your credit card at a physical location different from where you are.

---

[19] http://money.cnn.com/2017/09/15/pf/warren-schatz-equifax/index.html

Moreover, any credit bureau or data broker operating in Europe is already obligated to follow the more rigorous EU privacy laws. The EU General Data Protection Regulation will come into force, requiring even more security and privacy controls for companies collecting storing the personal data of EU citizens.[21] Those companies have already demonstrated that they can comply with those more stringent regulations.

Credit bureaus, and data brokers in general, are deliberately not implementing these 21st-century security solutions, because they want their services to be as easy and useful as possible for their actual customers: those who are buying your information. Similarly, companies that use this personal information to open accounts are not implementing more stringent security because they want their services to be as easy-to-use and convenient as possible.

9. This has foreign trade implications.

The Canadian Broadcast Corporation reported that 100,000 Canadians had their data stolen in the Equifax breach.[22] The British Broadcasting Corporation originally reported that 400,000 UK consumers were affected;[23] Equifax has since revised that to 15.2 million.[24]

Many American Internet companies have significant numbers of European users and customers, and rely on negotiated safe harbor agreements to legally collect and store personal data of EU citizens.

The European Union is in the middle of a massive regulatory shift in its privacy laws, and those agreements are coming under renewed scrutiny. Breaches such as Equifax give these European regulators a powerful argument that US privacy regulations are inadequate to protect their citizens' data, and that they should require that data to remain in Europe. This could significantly harm American Internet companies.

10. This has national security implications.

---

[20] https://www.cnet.com/news/equifax-trump-white-house-official-replace-social-security-numbers/

[21] http://adage.com/article/datadriven-marketing/eu-privacy-rules-complexity-data-marketers/301854/

[22] http://www.cbc.ca/news/technology/equifax-canada-breach-sin-cybersecurity-what-we-know-1.4297532

[23] http://www.bbc.com/news/technology-41286638

[24] https://www.equifax.co.uk/about-equifax/press-releases/en_gb/-/blogs/equifax-ltd-uk-update-regarding-the-ongoing-investigation-into-us-cyber-security-incident

Although it is still unknown who compromised the Equifax database, it could easily have been a foreign adversary that routinely attacks the servers of US companies and US federal agencies with the goal of exploiting security vulnerabilities and obtaining personal data.

When the Fair Credit Reporting Act was passed in 1970, the concern was that the credit bureaus might misuse our data. That is still a concern, but the world has changed since then. Credit bureaus and data brokers have far more intimate data about all of us. And it is valuable not only to companies wanting to advertise to us, but foreign governments as well. In 2015, the Chinese breached the database of the Office of Personal Management and stole the detailed security clearance information of 21 million Americans. North Korea routinely engages in cybercrime as way to fund its other activities.[25] In a world where foreign governments use cyber capabilities to attack US assets, requiring data brokers to limit collection of personal data, securely store the data they collect, and delete data about consumers when it is no longer needed is a matter of national security.

11. We need to do something about it.

Yes, this breach is a huge black eye and a temporary stock dip for Equifax—this month. Soon, another company will have suffered a massive data breach and few will remember Equifax's problem. Does anyone remember last year when Yahoo admitted that it exposed personal information of a billion users in 2013 and another half billion in 2014?

Unless Congress acts to protect consumer information in the digital age, these breaches will continue.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.

[25] https://www.reuters.com/article/us-northkorea-cybercrime/north-korea-hacking-increasingly-focused-on-making-money-more-than-espionage-south-korea-study-idUSKBN1AD0BO