U.S. Senate
Subcommittee on Privacy, Technology, and Law
October 4th, 2017 "Equifax: Continuing to Monitor Data-Broker Cybersecurity"
Testimony

Jamie Winterton
Director of Strategy
Global Security Initiative
Arizona State University

Chairman Flake, Ranking Member Franken, Members of the Committee - My name is Jamie Winterton; I'm the Director of Strategy at Arizona State University's Global Security Initiative. I would like to thank you, Mr. Chairman and Ranking Member Franken, for convening a hearing on this critical issue, and inviting me to participate.

The Global Security Initiative (GSI) is an interdisciplinary research hub at Arizona State University, built to address some of the world's most complicated and vexing security challenges - such as cybersecurity. Creating real-world, positive outcomes in security requires that we bring together disciplines from across the university – computer science, law, business, social science, the humanities and psychology, to name a few - and create partnerships that span the public, private, and academic sectors. GSI works closely with industry partners, and also serves as ASU's primary interface with the Department of Defense, the U.S. intelligence community and the U.S. Homeland Security Enterprise.

In my role as Director of Strategy at GSI over the past 3 years, I've helped craft ASU's approach to the important topic of cybersecurity. We created our Center for Cybersecurity and Digital Forensics with the express purpose of "advancing research and discovery of public value", as our University charter states. I work closely with our industry partners – some brand-new startup companies, some Fortune 100 - to understand the real-world problems they face. We design collaborative research projects that address these problems and build cybersecurity for everyone. I chair our University's DARPA Working Group, and work with faculty in creating lasting research relationships across the Department of Defense, Intelligence Community, and Homeland Security Enterprise. Specifically on the topic of cybersecurity, I've commented extensively in the media about ways individuals can protect their personal data, and have run a class on cybersecurity self defense (in collaboration with New America and Slate). Prior to my job with the University, I was a scientist at Lockheed-Martin for over a decade.

It's helpful to start any conversation on cybersecurity by defining the term. I think of "cybersecurity" as "protecting the points where human lives meet digital technology".

Our lives are deeply intertwined with the internet. Some of these ways are obvious – we sign up for a Twitter account, we buy things online, we search the web for information, we stream movies. But in those examples, the consumers are in control. Other points where human lives meet digital technology are beyond our personal control. Much of our personal information is collected by data brokers, such as Equifax. Credit monitoring companies play a unique and important role in our economy – they help lenders understand and mitigate risk while providing opportunities to consumers. But the extensive and highly personal data they store comes with an additional mantle of responsibility. The grave consequences of the data breaches that have motivated this hearing and others demonstrate that companies need to take these responsibilities more seriously.

Two years ago, a hearing was held in this room – a predecessor to our meeting today. It was titled 'Data Brokers — Is Consumers' Information Secure?' That hearing was motivated by a data breach at another credit reporting agency: Experian. In that breach, 15 million records were exposed, records that included names, dates of birth, addresses, Social Security numbers and drivers' license numbers. But we're back here today to discuss an event *nearly ten times as large* – 143 million records were exposed in the Equifax breach. That's nearly half the population of the United States (although some of the records do belong to non-US citizens).

What happened?

The media has covered the timeline of events extensively[1]. In mid-May of this year, hackers infiltrated the Equifax network, creating approximately 30 points of intrusion. In late July, the intrusion was detected. It wasn't until September that victims of the breach were notified – and we discovered that the vulnerability used to break into Equifax's sensitive databases could've been patched back in March.

But anyone watching the headlines knows that the Equifax breach is not an isolated event. Target, Home Depot, Sony, Anthem, the Office of Personnel Management - all experienced intrusions and loss of sensitive data. Just last week, Deloitte – the world's

[1] 'A Timeline of Events Surrounding the Equifax Data Breach'. Elizabeth Weise, USA Today, 26 September 2017. https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/#

largest cybersecurity consulting firm[2] - reported a breach that included all company administrator accounts and its entire internal mail system[3].

The question, then, is not just "What happened?" but also "Why?"

Threats are evolving more quickly than defenses. Companies collect and store vast amounts of personal data, yet cannot adequately protect them. One reason we can't sufficiently secure online systems is because we fail to understand their complexity – from a computer science perspective, a social science perspective, or a legal perspective, much less the overlap of all three. These are all areas that should be addressed by strong academic-industry partnerships in interdisciplinary cybersecurity research. This approach is also advocated by the Computing Community Consortium's cybersecurity task force in an upcoming post titled 'Data breaches: Time to implement a forward-looking research agenda'. It's clear that we need some revolutionary approaches to the problem if we want things to change.

To craft a research agenda that can solve the real challenges facing our nation, we must first understand the impacts of large-scale data breaches. Much of the discussion on this topic has centered on the individual impacts of the Equifax breach. This is both understandable and justified. People feel violated. They're exposed at a personal level. The response from Equifax has been lacking in both actionable content and empathy.

But I want to address an additional concern that this breach raises – a national security concern.

143 million credit records is an immense amount of data. We don't know who has that data now, or why they took it. Motivations could include identity theft or credit card fraud. But I want to talk about what a foreign adversary might be able to do with a data set that large. 143 million records – a data set that size allows a potentially hostile group to take an in-depth look into our economy and how it functions. These records aren't just numbers that determine whether or not an individual should get a loan. In combination, they paint a picture of our citizenry, one that could allow an adversary to understand vulnerabilities in our economic systems or in our society.

---

[2] 'Largest Cybersecurity Consultant Of the World Rocked By Cyber Attack'. Consultancy UK, 02 October 2017. http://www.consultancy.uk/news/14068/largest-cybersecurity-consultant-of-the-world-rocked-by-cyber-attack

[3] 'Source: Deloitte Breach Affected All Company Email, Admin Accounts'. Brian Krebs, 17 September 2017. https://krebsonsecurity.com/2017/09/source-deloitte-breach-affected-all-company-email-admin-accounts/

Chairman Flake, at your 2015 hearing on the Experian breach, you said "What may not be sensitive as one item may become sensitive in the aggregate". The national security concerns become even more concerning when you overlay the Equifax breach onto other large-scale breaches of sensitive information – like the breach at the Office of Personnel Management in 2015. Over 21 million security clearance files were exposed - social security numbers, birthdates, fingerprints, and SF-86 forms, and the accompanying interview notes. One prerequisite of holding a security clearance is having good credit. Bad credit – too much debt, or the inability to manage money – could leave a person vulnerable to blackmail or bribery by an adversary to "leak" classified information. A lot can happen in between clearance updates, though. Data from the Equifax breach, matched up with information from the OPM breach from just a few years ago, could potentially be used as a roadmap for vulnerable people in our security apparatus. That is a chilling scenario – but one that must be considered carefully as we design a new path forward.

At an Arizona State University event this past March, titled 'Unlocking the Privacy/Security Debate', former DHS Secretary Michael Chertoff addressed the issue of cybersecurity breaches, saying, "I think security and privacy are not only better together, I think they have to be together. They are two sides of the same coin. [Recent cybersecurity incidents] warrant a cool appraisal of where we are and where we need to be."[4] Having discussed where we are, I'd like to focus now on the last part – where we need to be.

In the cybersecurity industry, we call the offense the red team and the defense the blue team. And we have a saying: "Red team only has to be right once, but blue team has to be right every time." *This is an unsustainable condition*. Our current cybersecurity situation is like a person without an immune system – one small intrusion can cause massive effects that can shut down the system for considerable periods of time, and cause considerable damage. Our online systems are continually under attack, and it's unrealistic to believe that we can fend off every intrusion, every time. Cyber adversaries are clever and very persistent.

This is not to say that security is impossible. Clearly there are some "best practices" that must be followed to create a system that meets the minimum bar for security: enable two-factor authentication, develop a rapid patch management system, employ security-in-depth methodologies within the organization, encrypt data in transit and at rest. There are well-known, straightforward (although not necessarily trivial) ways to be a responsible

[4] 'Former Homeland Security chief speaks at ASU privacy-security forum'. Ashley Irwin, ASU Now, March 21, 2017. https://asunow.asu.edu/20170321-solutions-homeland-security-michael-chertoff-asu-privacy-security-debate

steward of personal data. But to ensure the security of our citizens beyond this event, we must now start thinking about how to address the big picture questions.

To quote Senator John McCain, from a cybersecurity congressional conference at Arizona State University this past summer, "the rapid development and deployment of information technology by American businesses and by our government has created new vulnerabilities. The entire information domain has become a potential battle space, and our enemies' methods encompass everything from straightforward data collection to hacking attacks that might disable critical national infrastructure."

The old methods of securing digital systems aren't working. It's time to think about the problem in a different way and take a new course of action.

We must begin building systems that can recognize an attack and defend against it, minimizing the damage of each intrusion – much like a healthy immune system isolates and destroys an intruding virus. Imagine a computer network that could identify an attack, separate the invader from sensitive data, and perhaps even mislead the attacker into giving up valuable information about his or her intentions, methods, or location. Instead of focusing exclusively on stronger perimeters, we need computer scientists, data scientists, and evolutionary biologists to research the question: *how can we design new systems that are reliable and resilient in the face of consistent attack?*

Another strategic issue we must consider is how we will securely identify people in the future. Most of us have gotten a letter at some point, notifying us that our data was exposed in a breach. It could've been from a credit reporting company, an insurance company, or a government entity – but at some point, it's probable that your data has been exposed. We can no longer rely on traditional methods of identification. Research in this area can create the secure identity of the future and help answer the question: *How can we develop new systems to uniquely identify people that will be robust, secure, and easy to implement, while simultaneously addressing privacy concerns of citizens?*

One area of research that has significant potential to reduce cyber risk is in human-computer interaction. Cybersecurity is not solely a technology problem – it's a technology-plus-human problem. In a recent blog post, Dr. Andrew Bernat, Executive Director of the Computing Research Association, stated that "In cyber-security work, where the human is often the weakest link in the chain, it is especially crucial to understand the varying motivations and usage patterns that dictate how people interact with their machines, and the expertise in studying those issues in large part resides in the

social, behavioral and economic sciences."[5] Every breach has human victims, but every breach is also perpetrated by human attackers, with human motivations and methods. *How do we better understand the interplay between people and technology, both defensively and offensively, in order to comprehensively secure the system?*

I am often asked about how regulatory groups like the FTC can and should approach large-scale data breaches – whether they should regulate on the front end, punish on the back end, or both. We can't start to meaningfully answer this question until we understand the true cost of a breach. There is currently no way to put a meaningful price tag on the exposure of 143 million credit records, either from an individual or national security perspective. In the days of the Target and Home Depot breaches – some of the first big public breaches – many thought that the price would be paid through consumer loyalty, or a hit to the stock price. The data hasn't shown that to be true. Through research in law, economics and risk analysis, we can start to answer the question: *How do we accurately and meaningfully calculate the cost of a breach, and how should regulators respond?*

These questions will only grow in importance, as critical infrastructure systems (such as energy and water) go online, as more internet-enabled devices enter the workplace and home, broadening the potential attack surface for an adversary. We're collecting more data every day, but our security practices aren't evolving. Incremental improvements won't work – to borrow a phrase from DARPA, the Defense Advanced Research Projects Agency, *we need a revolutionary - not evolutionary - approach*.

The nation's universities are already focusing on this critical issue. We are ready and able to partner with you. We bring deep subject matter expertise, long-term focus, and the ability to blend disciplines to create desperately needed solutions. We can focus our energies on understanding the long-term strategic issues, not just the important operational needs that companies face. We have an energized population of students and faculty who exist to solve problems. The next generation of cybersecurity experts will come through Universities, and it's important to give them real-world, hands-on research experiences. Getting those research experiences in college means they are already contributing to solving problems - they aren't just ready to join a workforce pipeline, they are already forming useful solutions. Universities have a culture of exploration; we embrace tough challenges and have the freedom to take risks. In these endeavors, we value our deep relationships with our industry and government partners – the challenges

---

5 'Why Social Science? Because It Makes Computing Work for People'. Andrew Bernat, Computing Research Association Bulletin, 12 September 2017. http://cra.org/social-science-makes-computing-work-people/

they face are real, we face them together, and we are committed to helping create solutions.

I am grateful for the work of Chairman Flake and this Subcommittee in addressing these important issues, and I thank you for inviting me here today.

Respectfully,

Jamie Winterton
Director, Strategy
Global Security Initiative
Arizona State University