Prepared Statement of Marissa Mayer
before the U.S. Senate Committee on Commerce, Science, and Transportation

November 8, 2017

Chairman Thune, Ranking Member Nelson, and distinguished Members of the Committee, thank you for the opportunity to appear before you today to discuss important issues surrounding consumer protection and data security.

I had the honor and privilege of serving as Yahoo's Chief Executive Officer from July 2012 through the sale of its core operating business in June of this year. As you know, Yahoo was the victim of criminal state-sponsored attacks on its systems resulting in the theft of certain user information. First and foremost, I want to reiterate how sorry I am for these incidents. We worked hard over the years to earn our users' trust, and we fought hard to preserve it. As CEO, these thefts occurred during my tenure, and I want to sincerely apologize to each and every one of our users.

When Yahoo learned of a state-sponsored attack on its systems in late 2014, Yahoo promptly reported it to law enforcement and notified the users understood at that time to have been directly impacted. Yahoo worked closely with law enforcement, including the Federal Bureau of Investigation ("FBI"), who were ultimately able to identify and expose the hackers responsible for the attacks. We now know that Russian intelligence officers and state-sponsored hackers were responsible for highly complex and sophisticated attacks on Yahoo's systems. On March 15, 2017, the U.S. Department of Justice ("DOJ") and FBI announced a 47-count indictment charging four individuals with these crimes against Yahoo and its users. In connection with the government's investigation, the DOJ and FBI praised Yahoo for our extensive cooperation and "early, proactive engagement" with law enforcement, as well as our

"leadership and courage," and described Yahoo as "great partners" in the government's multi-year investigation.

As part of our cooperation with the government to try to prevent these type of crimes, in November 2016, law enforcement provided Yahoo with data files that a third party claimed contained Yahoo user data. Yahoo worked closely with law enforcement and leading forensic experts to investigate and analyze that data. Following the investigation, Yahoo determined that user data was most likely stolen from the company in August 2013. Although Yahoo and its outside forensic experts were unable to identify the intrusion associated with the August 2013 theft, the company promptly disclosed the incident, notified users believed to have been affected, and took steps to secure all user accounts, including by requiring potentially affected users to change passwords.

The stolen account information included names, email addresses, telephone numbers, dates of birth, hashed passwords and, in some cases, encrypted or unencrypted security questions and answers. The stolen account information did not include unprotected passwords, social security numbers, or sensitive financial information, such as payment card data or bank account information.

Before I go on, I want to stress how seriously I view the threat of cyber attacks, and in particular state-sponsored attacks, such as those that victimized Yahoo and its users, and how personally and deeply I feel about these potential risks. After growing up in Wausau, Wisconsin, I remember buying my first computer in college, developing a passion for computer science and writing code, and seeing the potential for how this emerging technology could change the world. After college, my commitment to this field only grew after I was hired by a small start-up named Google as their 20th employee and first woman engineer. There, over the

next 13 years, I worked my way up from software engineer to Vice President of Search Products and User Experience, ultimately becoming a member of the executive operating committee.

In July of 2012, I became the CEO of Yahoo. As a pioneer of the World Wide Web, Yahoo was founded in 1994 as the hobby of two Stanford University students and over the next 20 years, Yahoo grew into one of only three internet companies in the world with more than one billion monthly users. Yahoo is a guide to digital information discovery, focused on informing, connecting, and entertaining users through its search, communications, and digital content products. I will always be grateful for, and humbled by, the opportunity to have led Yahoo and its employees for the last five years.

My experiences from Yahoo and Google have shown me the amazing potential of the internet to change our world for the better. They, however, have also reinforced the potential dangers posed by cyber crime.

With an increasingly connected world also comes a new host of challenges, including a dramatic rise in the frequency, severity, and sophistication of hacking, especially by state-sponsored actors. I am here today to discuss with the Committee, as best I am able, our efforts to confront the challenges of cybersecurity, including some of the security measures and defenses Yahoo had in place, in the hope of further advancing consumer protection and security. Please understand that the investigations regarding the Yahoo attacks remain active and ongoing, and there are limits on what I know and can discuss about the specific security events. Investigations into data security incidents often evolve over time and my statements today are based on, and limited to, information from my time at Yahoo.

Throughout my tenure as CEO, we took our obligations to our users and their security extremely seriously. We worked hard from the top down and bottom up to protect our

systems and our users. We devoted substantial resources to security – both offensively and defensively – with the shared goal of staying ahead of these sophisticated and constantly evolving threats. After I joined Yahoo, we roughly doubled our internal security staff and made significant investments in its leadership and the team. We hired strategically, filling our ranks with security specialists who focused on threat investigations, e-crimes, product security, risk management, and offensive engineering.

In addition to improving our talent, we also improved our security processes and systems defenses. Yahoo's security investments and initiatives included the adoption of a comprehensive information security program that enhanced our policies, procedures, and controls. Yahoo focused its program on the core National Institute of Standards and Technology Cybersecurity Framework functions: identify, protect, detect, respond, and recover.

Yahoo had in place multiple layers of sophisticated protection. Through cross-company initiatives like SSL and HTTPS end-to-end encryption, Account Key and multi-factor authentication, and password hashing and salting protections, Yahoo also helped bolster the company's security defenses and protect its users.

Recognizing that the best defense begins with a strong offense, Yahoo also adopted an attacker-centric approach to its information security program. For example, Yahoo staffed independent teams of some of the world's most sophisticated hackers to proactively attack our systems and report any vulnerabilities. Yahoo also formalized a "bug bounty" program, whereby the company pays security researchers who report vulnerabilities to the company. Since its inception, Yahoo's bug bounty program helped enhance and harden the security of our products. The bounties awarded by the company surpassed $2 million, with more than 2,500 security researchers participating worldwide.

During my tenure at Yahoo, we were extremely committed to our security programs and initiatives and invested tremendous resources in them. I want to thank all of our team members for their tireless efforts in addressing Yahoo security. As CEO, working with them over the past five years was nothing short of a privilege.

Unfortunately, while all our measures helped Yahoo successfully defend against the barrage of attacks by both private and state-sponsored hackers, Russian agents intruded on our systems and stole our users' data. The threat from state-sponsored attacks has changed the playing field so dramatically that today I believe that all companies, even the most-well-defended ones, could fall victim to these crimes.

I will close by saying that cybersecurity is a global challenge where the security threats, attacks, and techniques continually evolve. As we all have witnessed: no company, individual, or even government agency is immune from these threats. The attacks on Yahoo demonstrate that strong collaboration between the public and private sectors is essential in the fight against cyber crime. In addition, aggressive pursuit of cyber criminals, as the DOJ and FBI exhibited in Yahoo's case, could be a meaningful deterrent in preventing future crimes like these.

To echo the words of the then Acting Assistant Attorney General overseeing the investigation of the cyber crime perpetrated against Yahoo: a nation-state attack is not a fair fight, and it is not a fight you will win alone. By working together, we can help level the cyber playing field.

Thank you for the opportunity to address the Committee today. I look forward to your questions.