Opening Remarks of FTC Chairwoman Edith Ramirez
Start with Security
San Francisco, California
September 9, 2015

I am delighted to be here in San Francisco this morning to welcome you to the Federal Trade Commission's first "Start with Security" workshop. At the outset, I would like to thank Chancellor Wu and the University of California Hastings College of the Law for co-sponsoring this event and hosting us today. I also want to acknowledge the FTC staff who organized this program, as well as express my gratitude to the speakers who are joining us today to share their insights and expertise.

A few blocks from here, Apple is unveiling its newest products. Here we have a launch of a different kind – the launch of the FTC's "Start with Security" initiative. As the chief federal agency charged with protecting consumer privacy, the FTC strives to help promote a marketplace where innovation flourishes, while also ensuring that consumers' personal information is safeguarded. As part of our "Start with Security" initiative, we are hosting workshops like this one across the country to provide practical guidance to small and medium-sized businesses to help them implement security best practices.

Our focus today is on how tech start-ups and developers can integrate security into their products and services. Start-ups are not only an important engine of growth in today's economy, but also crucial partners in our effort to keep our marketplace secure.

Through your innovative software products and services, you are transforming the lives of millions of consumers. Thanks to your entrepreneurship, we can instantly hail a ride, optimize our energy use, and automate our homes using connected devices. Thanks to you, we can track our fitness goals, send health updates to our doctors, and even contribute to medical research through the devices we wear. The software revolution has left little untouched, with tremendous benefits to consumers and society as a whole.

But in a world where everything is connected, insecure products and services can have significant consequences. In recent months, we have heard about online dating service breaches that exposed users' intimate information, the theft of digital currency through attacks on bitcoin exchanges, and the hacking of vehicles that could place lives at risk. It has never been more clear that we must secure the software supporting our digital lives.

The tech industry is critical to this effort. Innovation begins with you, but so too should security. As start-ups, you spend much of your time thinking about raising capital, securing patents, or increasing your marketing. But the security of your products can also play an important role in the success of your business and widespread consumer adoption. The consequences are very real when consumers' privacy and security are compromised. It is bad for business, and bad for consumers. Your presence here today underscores your commitment to prioritizing security.

I. FTC Enforcement

Before I turn to how you can build in security from the start, let me briefly describe the FTC's privacy enforcement program. To protect consumer privacy, the FTC brings law enforcement actions against companies of all sizes in both the online and offline arenas. We have taken action against social networks, pharmacies, and mobile app developers, among others. Through our enforcement, we aim to ensure that companies make truthful representations about their privacy and security practices, and that they provide reasonable security for consumer data.

Unfortunately, as our cases demonstrate, not all companies have implemented reasonable security measures to protect consumer information. Indeed, our cases have addressed a range of security failures. For example, in our action against Snapchat, we alleged that the company's failure to secure its "Find Friends" feature resulted in a security breach that allowed attackers to access the usernames and telephone numbers of 4.6 million consumers. In a case against Credit Karma, a mobile app start-up, we alleged that the company made deceptive representations about the use of SSL encryption to secure the transmission of consumers' sensitive information, leaving them vulnerable to "man-in-the-middle" attacks. The lesson from these and other FTC cases is clear: in the rush to innovate, privacy and security cannot be overlooked – even in the fast-paced start-up environment.

II. Building a Culture of Security

So how can start-ups and developers avoid these pitfalls? How do you build a culture of security from the start? Our business guidance on protecting personal information,[1] building mobile apps,[2] securing connected devices,[3] and starting with security[4] include a number of practical recommendations, but I would like to highlight three key steps that you can take to integrate security into your products and services.

[1] *See* FTC Business Center, *Protecting Personal Information: A Guide for Business* (Nov. 2011), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[2] *See* FTC Business Center, *Mobile App Developers: Start with Security* (Feb. 2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

[3] *See* FTC Business Center, *Careful Connections: Building Security in the Internet of Things* (Jan. 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things.

[4] *See* FTC Business Center, *Start With Security: A Guide for Business* (June 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

First, think about privacy and security as you design your product – embed it into the development process. For instance, when you develop an application, consider what information it will collect, how long you will retain it, how you will use it, and how you will secure it. These decisions could reduce the risk of a breach down the road. If your app is transmitting usernames, passwords, API keys, or other important data, use transit encryption. If you are using a library or software developer kit to build your app, research whether it has known security vulnerabilities. And train your engineers in secure coding to avoid vulnerabilities in the design of your software. All of these steps can help you build a secure product from the start.

Second, test your product. Are security defaults operating as intended? Are the choices that you offer to consumers working? Are the controls you have implemented secure? Evaluate your product in scenarios that replicate how consumers will use it in the real world. Often, there are financial incentives to rush to market, but make sure your security is ready before you launch.

Third, bugs are inevitable, and when flaws are discovered, companies must have effective strategies for managing, addressing, and learning from vulnerability reports. Consider setting up a bug bounty program or a contact point for receiving vulnerability disclosures from the security community. In addition, software libraries often require security updates. Once you launch your product, security must still be a priority.

The FTC's "Start with Security" guide – which we are distributing today – can help you identify, and possibly prevent, these and other security pitfalls.

III. Workshop Overview

You may wonder how a start-up that is bootstrapped for resources, growing at breakneck speed, and continuously pushing code can implement these practices. How can security be adapted to such a dynamic, fast-paced environment?

To answer these questions, today's workshop will focus on creating a secure app development lifecycle. That lifecycle has many phases – building a culture of security from the start by embracing "security by design," adapting security testing in high-growth settings, and developing a plan for responding to vulnerabilities. Our exchange today will leverage the expertise of tech industry experts, as well as the FTC's own enforcement experience, to identify practical ways that each of you can build secure apps.

You will hear from security engineers who have built security programs at high-growth start-ups like Dropbox, Etsy, Pinterest, and Twitter. You will also hear from experts at platforms like HackerOne that help companies of all sizes create the kinds of security programs once reserved for only the largest tech companies. From securely designing and coding your apps to engaging with the security community when bugs are discovered, you will hear practical guidance on how to integrate security into your app development lifecycle. The culture of security that these experts will describe is essential to the continued growth of the tech industry.

We hope that you will spread the word about the importance of security, and the potential negative consequences – from customer backlash to negative press attention to potential exposure to FTC enforcement – of ignoring security concerns.

IV. Conclusion

To close, I want to emphasize that by adopting security best practices in your organization, you can ensure that your products and services are trustworthy. So while your motto may be “Move fast and break things” or “Think different,” I would also urge you to take a step back and implement your creative and disruptive ideas responsibly. As you innovate, keep in mind that you are also stewards of consumer data, that the loss of that data could have disastrous consequences, and that, to avoid these consequences, you have a responsibility to start with security.