



May 30, 2014

Hon. Donald S. Clark  
Federal Trade Commission  
Office of the Secretary, Room H-135  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

*VIA ELECTRONIC FILING*

Thank you for the opportunity to submit this comment on mobile security, including Android's efforts to ensure that our users enjoy our open mobile platform without compromising their data security. I appreciated participating as a panelist at the Federal Trade Commission's workshop, "Mobile Security: Potential Threats and Solutions," and hope that this comment further assist the Commission's analysis of data security issues.

We welcome discussions about the security of any of our products. We also believe that policymakers should focus not just on mobile but on data security issues across the spectrum. When stakeholders approach data security holistically, rather than in sector-based or technology-specific silos, consumers and companies can make better security investments to protect themselves from the most pressing threats. As the Commission [reported](#) earlier this year, identity theft has been the top complaint of consumers for 14 straight years, and these crimes often stem from data security attacks across all types of platforms and devices, as hackers and fraudsters target consumers directly or attack the corporate networks that hold their data.

Accordingly, we agree with [consumer advocate groups that have called](#) on the Commission to conduct a broad public analysis of data security. Doing so would allow the agency to determine and report on where the risks to consumers are most clear and demonstrated, what practices are being utilized to combat these threats, and what guidance might have the most beneficial impact on user security. As described below, mobile security is just one piece of the data security landscape, and consumers are more likely to be harmed by security threats across the Internet and other platforms.

In this comment, we highlight a few of our key innovations and approaches on Android, and we encourage the Commission to review the comprehensive overview of our publicly available [Android security model and processes](#) at the Android Open Source Project Website. In addition, we

encourage the Commission to focus holistically on data security. Such a policy approach would best address the concrete harms facing consumers from data breaches and other security threats.

## **Google's layered security approach**

The security and privacy of all of our users' data is of primary importance to Google. We employ over 400 engineers and other experts to keep our users' data safe and secure across all our products and services, including our Android platform. We are dedicated to building, maintaining, and protecting all of our platforms and services with state of the art security, and our efforts to protect our mobile users is no exception.

At Google, we take an integrated approach to security management across our various platforms, services, and devices. We look at threat vectors across devices, platforms, and user experiences, rather than using a siloed approach that would place artificial boundaries on threats that bad actors themselves aren't limited by. For example, we use our deep experience in identifying malware across the Internet, such as through [Safe Browsing](#), to combat the next generation of malware threats regardless of how and where they may arise.

In general, Google uses a "defense-in-depth" approach to protecting consumers with multi-layered security to prevent any one system from becoming a single point of failure. We employ a combination of automated tools and manual review to keep our services secure and detect any abuse or suspicious activity in our system environment. Of course, an integral part our layered approach is to design security and resilience into our products and platforms from the ground up.

Our Android users are protected through this kind of holistic approach. For example, we work hard to leverage our long-standing experience dealing with malware threats in all types of software to protect our Android users.

- **Google Play's** application scanning tool performs as an automated review of all applications in the Play Store to keep potentially harmful applications out entirely. We analyze newly uploaded applications, applications already in Play, and developer accounts. An application will get analyzed many times in its life cycle -- newly uploaded applications are analyzed immediately for harmful behavior such as that commonly described as malware, spyware and trojans, and previously uploaded applications are periodically analyzed as well. This automated review looks for behaviors that indicate an application might be potentially harmful, and compares it against previously analyzed applications to detect possible red flags. We run every application on Google's cloud infrastructure and simulate how it will run on an Android device to look for hidden, malicious behavior. We also analyze new developer accounts to help prevent malicious and repeat-offending developers who have been banned from coming back.
- **Verify Apps** is an extension of Google Play available to most Android users for free that allows consumers to verify applications in order to help prevent harmful software from being

installed on their device. This verification service will screen applications prior to installation regardless of the source from where they are downloaded. If an application is deemed potentially harmful, Google will warn users that they may not want to install it, while applications that are known to be harmful will be blocked entirely. In the last year, Verify apps has been used more than 4 billion times to check apps at the time of install. Earlier this year, we [announced](#) the roll out of a new enhancement to extend this protection even further by *continually* checking devices to ensure that all downloaded applications are behaving in a safe manner, even after installation.

- **Sandboxing** is an operating-level technique used by Android to put virtual walls between applications and other software on the device. If users download a malicious application, that application will not be able to access data on other parts of their phone and the potential harms would be limited. Sandboxing is also used in Chrome and Chrome OS in order to ensure that a malicious page cannot impact a user's computer or other services.
- The **Safebrowsing API** is an extension of this application review to applications across the open web, including many third-party markets. The Safe Browsing service is provided by Google to enable applications to check Google's constantly updated lists of suspected phishing and malware pages on behalf of their users. As a result, software and website developers using the service can warn users before clicking on links that appear in their applications when they lead to malware-infected pages, can prevent users from posting links to known phishing pages from the developers' software or website, and check a list of pages against Google's lists of suspected phishing and malware pages.

Of course, application developers play an important part in maintaining the security of Android. We provide Android developers with a rich [security model](#) for them to use to best protect their own users, with a robust set of recommendations to build security into the creation of new applications. We also provide developer education on security, such as sessions on securing user data at our annual developer conference Google IO. Recently we have taken an even more aggressive approach to helping developers build secure applications by providing developers with a warning if they submit an application to Google Play that includes a potential security vulnerability.

### **Strong security through openness**

Google's layered approach also depends on the openness of our many platforms, including Android. Consistent with our long-standing support for an open and secure web, Google believes that the online experience -- whether accessed through a desktop, laptop, Android web browser or through apps -- should be both open *and* secure. History has shown that open platforms have consistently created significant beneficial content for consumers over the long term while also creating strong security environments.

The history of open source and our own experience with Android, Chromium, and other open source projects makes clear that openness fosters fewer vulnerabilities than closed approaches.

Some have wrongly viewed open source as inherently less secure or easier to hack than “closed” software. However, our open platform allows for the entire Android community, including developers, security experts, and other stakeholders to analyze potential threats and learn from each other to further decrease the risks of security threats on the Android platform.

Our open approach allows us to actively encourage the highly engaged developer community to scrutinize the source code, and offer suggestions about how to tighten up the security infrastructure. In addition, our open code also allows for considerable research of security experts, which we welcome -- we believe that there is more security research performed on Android than any other mobile platform. In addition to the considerable research by Google and Open Handset Alliance partners, the open nature of the Android platform has provided academics and industry with broad and deep access. In addition, we have worked to spur these efforts through innovative programs to encourage research, such as our [Patch Reward Programs](#) that incentives researchers to develop security improvements across our popular open source projects, including Android. As a result, our open platforms allow us to constantly learn from the research of others about new threats and vulnerabilities, and not just rely on our own research.

While assuring the security of the Android platform, we are still able to also create an environment that allows developers to flourish in creating great products for consumers. For example, Google incorporates automated review, rather than relying on manual curation, to allow new application developers to enter the marketplace quickly to begin competing with existing offerings. This scalable approach becomes increasingly important given the explosive growth of applications. Thus, Android proves that pro-competitive openness and superior security are not mutually exclusive.

## **Reacting to rare threats**

As a result of our layered approach, Android users are rarely affected by potentially harmful apps. We have made great efforts to secure Android and Google’s other platforms, and our security team works hard to find new bugs internally and responds quickly and professionally to vulnerability reports from external researchers. Once we learn about potential vulnerabilities, we move swiftly to patch them, and we also move quickly to eliminate potentially harmful apps from the Play Store and devices using Verify apps once new threats have been identified.

Ultimately, the entire Android ecosystem is being well managed by platforms, service providers, and the broader mobile industry. Because bad actors have always tried to stay one step ahead of those working to protect users, we work with many stakeholders to both identify new threats and incorporate this knowledge into our defenses.

## **A holistic approach of data security**

Finally, it is important to note that data security does not exist in silos. Because consumers face security threats across computing and payment platforms, as seen from the continual drumbeat of new data breaches, Google treats data security in a holistic manner. Whether they be point-of-sale

attacks, hacking of corporate networks, hijacking of consumer online accounts, or many of the other types of data security problems, it's clear that the threats vary across devices and platforms. Indeed, many of these threats overlap, as hackers can attack through multiple vulnerabilities.

Given that the threats are not specific to any type of device or platforms, our approach to data security vulnerabilities are not either. Many of our anti-malware efforts described above or employed throughout the Internet ecosystem can and should apply regardless of the type of device, platform, or software at issue. We use automated security scanning on a variety of our products to protect consumers on whatever device they use, and the lessons we learn in one area are used to improve security and fight fraud across the entire spectrum of Google's platforms, devices, and other user experiences.

Indeed, computing platforms are quickly converging and interoperating in ways that belie technology-specific approaches. For example, "mobile" is quickly becoming a distinction without a difference, as all devices are incorporating features that consumers love most, such as app downloading. In fact, existing mobile operating systems could be used across the spectrum of consumer devices, further eroding the distinction between mobile and non-mobile devices. Thus, data security should be approached by everyone in a technology-neutral manner, rather than adopting artificial distinctions that will not hold up in the near term.

## **Conclusion**

While we work hard to create technological tools to protect our users, we believe that security is beyond the reach of technology alone and requires a blend of technology, public policy, and industry engagement. Security is ultimately a shared responsibility, and Google is focused on developing technology to protect users across the web, contributing research, facilitating industry initiatives and conversations, and empowering users through security education. Our multi-layered approach depends on not just technology, but also learning from our own experience across all of our products and engaging with all stakeholders using and researching our open platforms.

Our multi-layered approach also depends on policymakers who engage with us across the spectrum of data security risks facing consumers. Rather than overemphasizing any specific category of security to the exclusion of the many different threats to consumers, we should all look across platforms, devices, and experiences to address risks everywhere. Accordingly, we hope to continue our engagement with the Commission across the entire data security landscape where consumers are most at risk.

Hackers and fraudsters attack consumers, businesses, and government entities from a variety of threat points, stealing identities, defrauding the government, and engaging in other criminal activities. These attacks cost our economy millions of dollars each day and shake our users' trust in the digital ecosystem. We commend the Commission for this important inquiry into security threats to consumers' devices, in what should be just one step in a continuing broad look at the many data security threats facing consumers.

\* \* \*

We thank you for the opportunity to provide this comment on this important subject. Please do not hesitate to contact us if you have any additional questions.

Sincerely,

Adrian Ludwig  
Android Security, Google