Testimony

of

Jonathan Zuck
President
ACT | The App Association

before the

Committee on the Judiciary
The Subcommittee on Courts, Intellectual Property and the Internet

on

Chapter 12 of Title 17

September 17th, 2014

1401 K Street NW Suite 502
Washington, DC 20005
202.331.2130
@ACTonline
ACTonline.org
/actonline.org

Chairman Coble, Ranking Member Nadler, and Members of the Subcommittee, thank you for the opportunity to speak today about an important area of copyright law and its impact on the app industry. Let me first say that we appreciate your continued leadership in the process of reviewing the effectiveness of the U.S. Copyright Act to protect intellectual property rights, encourage creativity and innovation, and provide consumers with legal access to content in the digital environment.

ACT | The App Association represents over 5,000 app companies and information technology firms creating and licensing digital content. ACT is widely recognized as the foremost authority on the intersection of government and the app economy. As the only organization focused on the needs of small business entrepreneurs from around the world, ACT advocates for an environment that inspires and rewards innovation while providing resources to help its members leverage their intellectual assets to raise capital, create jobs, and continue innovating.

The App Industry

This is a success story. A story about a vibrant, innovative, and growing industry that is in every congressional district in the United States.

The app industry is growing rapidly as mobile devices are where remarkable innovation is taking place. After the launch of the first app store just six years ago, apps have grown into a $68 billion industry and created over 750,000 U.S. jobs. Industry analysts expect revenues to grow to more than $140 billion by 2016.

The app ecosystem consists of a wide range of products and services, much like traditional copyright industries. These include a variety of content delivery options, security and monitoring services, tech support services, payment processing services, patents, licensing agreements, and diverse revenue models.

App Developers and the DMCA

The app industry as we know it today didn't exist when the Digital Millennium Copyright Act (DMCA) became law in 1998. At the time, software developers engaged in the debate over the proper balance between protecting content and not harming emerging and future innovations in technology. They understood the value of intellectual property to their ability to see a return on investment, still their technical expertise made them wary of the potential impediments to innovation and abuses which many argued would be the result of the DMCA. Despite some lingering concerns over the DMCA, software developers soon took advantage of opportunities to innovate in digital technologies, delivering content to consumers across the mobile ecosystem.

The DMCA is extremely technical and easily misinterpreted or misunderstood. Too often the law is debated without the participants having read the law or having any knowledge of what it does. And this impacts policy makers who are new to the issue, making it difficult to determine the facts versus the spin.

Realizing that there was a need to educate policy makers and the developer community about what the DMCA really does, ACT published a white paper on the 15th anniversary of the law last year entitled, "Quick Guide to the DMCA: The Digital Millennium Copyright Act Basics." It was time to dial down the rhetoric and focus the

debate back on the facts. The Quick Guide took out the legalese, provided context for why it was enacted, and explained how it works. It can arm policy makers with easy-to-understand facts about what the law actually says and its impact on innovation. And it shows developers they do not need to fear the DMCA but rather use it as an important consideration in their product development as both creators and users of content.

The Quick Guide broke down the two main sections of the DMCA: Section 1201 anti-circumvention rules and the online service provider liability provision. Focusing on section 1201, the Guide explained how the law provides copyright owners with the authority to prevent "circumvention" or breaking of technological measures or digital locks used to protect their rights under copyright law. App developers increasingly identify themselves as content creators as well as technological innovators. Seeing the value of being able to use security measures to protect access and use of their content has led to strong support for the DMCA amongst ACT members.

The Guide also refuted the main criticisms leveled at the DMCA since its passage with the overwhelming evidence of advances in technological innovation. Simply put, the worst fears of DMCA opponents did not materialize. While neither copyright owners nor tech and user groups were completely happy with the final language in the DMCA, it has proved to be flexible during the breathtaking digital revolutions of the past decade, which have brought us iTunes, smartphones, app stores, digital books and magazines, online access to art, YouTube, Hulu, and all sorts of other on-demand content.

Critics continue to claim that the DMCA "chills innovation," pointing to a handful of cases as proof. However, in each of these few cases, the courts have applied the facts and found that the DMCA either did not apply or was not violated. The courts have consistently and repeatedly rejected efforts to abuse the DMCA and new businesses and business models built around copyrighted content are flourishing.

DMCA opponents also argue that the DMCA gave too much control to creators claiming that content owners would and do limit access and raise prices. Again, products, services, and content offerings continue to grow exponentially while the costs to consumers continue to decline, and in many cases, are now free with the advent of ad-supported business models that are common in the app industry. There are thousands of apps available to consumers at price points of $0.99 or less.

But, lawmakers drafting the DMCA understood concerns about users having access to digital copyrighted works for legitimate uses, and specifically included a provision to ensure access for lawful purposes, like fair use. Every three years the Librarian of Congress, upon the recommendation of the Register of Copyrights, exempts certain types of works from the section 1201 rule against picking locks. And every three years the process has resulted in exemptions to the rule. While ACT has not participated in the process, we have observed that the procedure works. It is another example of the flexibility of the DMCA to adapt over time to meet the current needs of consumers and content owners.

ACT continues to use the Quick Guide to educate its members, the developer community, and policy makers about the DMCA. Focusing on facts, the Guide transforms the DMCA from a virtual boogeyman into a critical tool that is essential to the protection of content and continued innovation.

Securing Digital Content is Essential to Mobile App Industry

As much as I would like to report that piracy no longer exists, software developers still face significant loss of time and money from those who would rather steal than pay $1.99 for software that changes their lives. Worse still, the problems from pirated apps are not limited to obvious monetary damages. We now see more sophisticated thieves that steal the content and functionality of an app, and then submit it to a legitimate store under a different name – almost like fake brake pads that come in factory boxes. Additionally, these pirated apps are often vectors for malware and identity theft. Therefore we continue to need the tools provided by the DMCA as well as strong cooperation within industry between device manufacturers, platforms, and publishers.

It's worth remembering that copy protection for software at the time of the DMCA's passage was often an arduous, and individual, activity. Each publisher would create, manage, and update a copyright protection scheme, and smaller independent publishers would buy "kits" that would install on top of their software to offer protection. In both cases, copy protection was merely an arms race – with constant updates a reality that cost time, money, and focus.

For example, in 2005, one independent game developer in upstate New York, Ambrosia Software, reported that just to keep up with hacked codes, they had two employees that would start every morning, and spend more than two hours each day, merely cataloging all the codes on the web, and then one full time employee was dedicated to managing the legitimate owners so that once their stolen code was deactivated, they could get a new, working code.

Worse still, these copy protection methods would often lead to a bad user experience that required keeping a folder full of scraps of paper with code numbers and "authentication certificates" just to re-install your software. For developers and publishers, it meant customer support via phone and email available 24-7 if possible, and five days a week at minimum.

With the advent of the modern app store, we entered into an era where the app platforms now handle the bulk of the work, making it much easier to keep paying customers happy and keep thieves away.

How We Work with Platforms Today – and What are the Pitfalls

The modern app store revolutionized how developers handle piracy. Now stores would take care of the purchase, and validate that the right person got the right software. So long as the device was able to maintain its own internal security, traditional piracy became much harder.

As the app industry grew, we developers worked hard to find new ways to provide features that customers wanted, but only paid for when they were needed. This resulted in significant growth of "freemium" apps. These are applications that can be downloaded for free, but certain features or types of use are only available for purchase via an in-app purchase. Therefore, while you may not restrict the initial download, you must use anti-cracking techniques to protect the paid feature set. For mobile platforms like Apple's iOS, Microsoft Store, and Amazon's Kindle, developers of paid and freemium apps rely on the concept of the receipt.

The receipt is the foundation upon which developers build business model enforcement logic directly into the app, as well as into servers that are providing the content to users. Moreover, this digital receipt is a fairly similar analogy to the paper receipt you get from a store when you purchase a tangible good: It verifies the product you purchased, the method of purchase, if you used a credit card, who purchased it, and when the purchase happened. And just like Costco asks to see receipts as customers walk out, it also is a method to prevent theft.

For today's mobile and on-line platforms, those receipts are protected by digital rights protection mechanisms and are the trusted and verifiable record of purchase.

Unfortunately, easy-to-use digital rights management techniques like receipt validation haven't killed off piracy entirely. We still see sites and sources like pp25 and ihacksrepo on Cydia for iOS; aptoide and BlackMarketAlpha for Android; and the Modembreak hack for Windows Surface. And nearly all of these rely on breaking the rights protection built into the device—often called "rooting" or "jailbreaking."

In most cases these sites give users access to pirated software, but they also do something far worse—they flood the ecosystem with malware.

Copycat Apps and Malware – The Next Threat for Developers

Traditionally, we think of piracy as an end user getting ahold of software they haven't paid for and using it. Today, we see a rising form of piracy where a developer, nearly always overseas, steals the content and functionality of a legitimate product and then attempts to put it in the store under a new name—even charging users for the app!

In one recent example, an ACT member had a children's app in the GooglePlay app store for sale at $0.99. This fun kids' app, Zoo Train, is full of colorful animal shapes and fun animation for an audience of young children. During a search for the product, the developers found another app in the GooglePlay store, with their same name, using their artwork, but from a different publisher. This app was free in the store, and came up when you searched for the Zoo Train app.

Why would someone do something like offer a free version in the store with no clear upside? Well, this particular act of piracy was a two-front attack. To start with, the app didn't really work at all. Instead of working properly with puzzles and spelling lessons, it showed advertisements to earn bogus ad revenue, and then gained permission to take control of the user's device—including access to the phone dialer, the address book, and the network stack, and then set itself so it could run in the background. In short, it was set up as a malware "stub" that does nothing right now, but can be activated with an update and a command.

Unfortunately it took nearly a year for Zoo Train to get that malware app off the GooglePlay store. And they aren't alone. RiskIQ, an online security services company, estimated that there were more than 42,000 apps in Google's store containing spyware and information-stealing Trojan programs by 2013[1].

[1] http://www.businesswire.com/news/home/20140219005470/en/RiskIQ-Reports-Malicious-Mobile-Apps-Google-Play#.VBZ6UEsrhg1

Another ACT member reported 10,000 active, registered users on a discussion board about his app in a country where he had only seen two actual downloads.

We have even had reports of free, ad-supported apps being pirated. In these cases, the content and the functionality is stolen, with another ad network or payee slotted in underneath the stolen content. This technique shows that even giving software away doesn't defeat piracy.

What's worse about these copycat apps is that the user doesn't know. If the pirated version is downloaded from a seemingly-legitimate store, the user may be fooled into thinking he has paid the legitimate developer, and even call up the actual app publisher's customer service when it doesn't work right.

While this may sound like a laundry list of doom and gloom, I must report that overall developers and software publishers are finding the world of apps to be far better on piracy than the past. But the persistent problems created by piracy continue to nip at our heels.

Conclusion

Section 1201 of the DMCA created the foundation for protecting copyrighted works in the digital world. It's the result of a complex series of negotiations and compromises between policymakers, copyright interests, tech firms, network operators, and nonprofits. The final law is not without flaws, but it has proven effective and flexible enough to provide for and deal with continued innovation in the tech sector. The reality is that entrepreneurs have and will continue to find a way to build legitimate businesses without running afoul of the law. There may be opportunities to continue to improve the law to ensure it's ready for the next generation of technological advances, but we should be wary of dismantling a series of compromises that has served innovation and creativity well for the past 16 years.