Protecting Small Business Innovation

Monday April 2, 2012

Response by the Association for Competitive Technology to

Department of Commerce, Request for Comment

Docket No. 120214135-2135-01

The Association for Competitive Technology (ACT) is an international advocacy and education organization for people who write software programs--referred to as application developers. We represent nearly 5,000 small and mid-size IT firms throughout the world and advocate for public policies that help our members leverage their intellectual assets to raise capital, create jobs, and innovate. Our members are at the bleeding edge of the mobile apps ecosystem, and are primarily responsible for its continued success. In simple terms, the difference between a phone and a "smartphone" is the "smart" apps that run on it.

ACT is committed to the multi-stakeholder process as a way to improve industry efforts to protect consumer privacy. We recognize that consumer confidence in the safety of user privacy is necessary for app makers to effectively market their products. We will continue to work through this process, and with the members of the broader Internet ecosystem, to improve these efforts.

Specifically, app developers have three key messages for the National Telecommunications and Information Administration (NTIA):

1. **The app marketplace is still in its earliest growth stage, rapidly continuing to evolve.**

2. **The best way to address consumer privacy concerns is through a multi-stakeholder process producing voluntary, but enforceable, codes of conduct. However, we should avoid regulating technology instead of behavior and promote conditions to encourage the free exchange of ideas.**

3. **App developers and industry organizations are adopting measures to improve consumer privacy protections and increase awareness of the potential uses of personal information.**

ACT urges the NTIA to rethink its request for comment regarding a privacy process that will" convene an initial multi-stakeholder process … for mobile device applications". Targeting apps -- a single technology -- outside the general framework of the process is troubling and a cardinal sin of technology regulation. Isolating the industry sector composed primarily of small businesses disproportionately favors the larger companies that have repeatedly given consumers the most reason to be worried about their privacy.

Finally, we believe that setting up an initial process around "mobile apps" creates the impression that mobile is not only the most important front, but also the only area that needs addressing within the privacy realm. We fully understand this is not the intent of NTIA, but by focusing on technology collection and delivery mechanisms rather than data itself, the broader world audience is led to the conclusion that mobile is the only issue.

Evolution of the App Marketplace

Just two years ago, total industry revenues for mobile apps were $3.8 billion and expected to rise to $8.3 billion.[1] At the close of last year we had grown to $20 billion and are projected to reach $76 billion by 2015.[2] This is a meteoric rise for an app economy that didn't even exist four years ago.

This is also a small business phenomenon. Over 88 percent of the top 500 app makers are small businesses.[3] And as small business is the engine of economic growth in our country, app makers are contributing greatly to the job market with half a million jobs created in this new marketplace.[4] These jobs can be found anywhere. Thirty percent are in the state of California, but the rest are spread out across the country.

As a brand new industry, we are experiencing rapid changes in the marketplace with new business models emerging every year. Recently freemium apps and in-app purchasing have become the favored means to monetize new releases.[5] Not long ago, paid downloads ruled the day. Through it all, developers are still exploring whether the advertising model can generate enough income on its own. [6]

While business models continue to evolve, developers are also experimenting with different platforms. Currently Apple's iOS provides the most dependable platform, but RIM

[1] http://www.eweek.com/c/a/Mobile-and-Wireless/Apple-Google-Lead-38B-Mobile-App-Charge-IHS-512817/
[2] http://www.slideshare.net/joelrubinson/an3-us-appeconomy20112015
[3] http://Republicans.EnergyCommerce.house.gov/Media/file/Hearings/CMT/100511/Reed.pdf
[4] http://www.technet.org/new-technet-sponsored-study-nearly-500000-app-economy-jobs-in-united-states-february-7-2012/
[5] http://www.nytimes.com/2012/03/19/technology/game-makers-give-away-freemium-products.html?_r=1&pagewanted=all
[6] http://tech.fortune.cnn.com/2011/11/21/piper-jaffray-android-app-revenue-is-7-of-iphones/

has been aggressively wooing developers to Blackberry as its userbase in Asia and the Middle East remains strong.[7] Android continues to gain marketshare, though the platform suffers from fragmentation; and with dramatic changes coming in the new Metro user interface of Windows Phone 8, many software developers are porting their programs to that new mobile platform.[8]

With such a dynamic mobile ecosystem it is difficult to predict where the market is headed next and what industry standards will be adopted. This makes it difficult to implement a regulatory regime for the app marketplace. The industry is far from mature and activities or practices that regulators seek to address may no longer exist in their current form by the time new rules can be implemented.

Focus on Data Rather than Technology: A Framework for Workgroups and Products.

Understandably, NTIA is looking for someplace to start the multi-stakeholder process. We recommend NTIA start with focusing on **data collection, retention and sharing** across all platforms and devices. Within the data context we view this effort mapping to the seven objectives outlined in the Consumer Privacy Bill of Rights. Therefore we propose the NTIA structure the workgroups around the three key elements of data, and that each workgroup have subgroups that focus on a specific deliverable "best practice" or set of definitions that would then be moved up to the full workgroup, and eventually to the entire multi-stakeholder effort.

We propose the following structure and deliverables for each issue area and subgroup:

1. Data Collection Working Group
    a. **Individual Control**. Best practices around "Individual Control" of Personal Information (PI) data, including at what point does that data no longer belong to the individual? What level of de-identification is necessary?
    b. **Transparent.** Best practices regarding "Transparent" disclosure of information being collected – what are the time and space parameters industry should achieve to reasonably expect consumers have the opportunity to be informed?
    c. **Context.** Create a framework to determine at what point is PI not PI? Best practices regarding what information qualifies as PI, and does the collection

[7] http://www.engadget.com/2012/02/03/RIM-free-BlackBerry-Playbook-Android/
[8] http://www.reuters.com/article/2012/03/20/mobile-developers-idUSL1E8EJAGT20120320

and merging of multiple bits of non-PI data result in a "profile" that requires the same best practices as PI?

d. **Security.** Data determined to be PI should be collected in a manner in which customers have the same expectation of security regardless of platform. These specific characteristics require the establishment of best practices.
e. **Focused Collection.** Best practices that allow for focused collection, but also allow for broader data collection that may serve other purposes such as the improvement of an application or service.

2. Data Retention Working Group
    a. **Transparency.** Establishment of clear notification best practices to inform consumers about the length of time data is retained, how is it retained (as PI? Anonymized? Aggregate only?) and what definitions for terms including PI, Anonymized and Aggregate are applicable.
    b. **Context.** Mapping to "Context" in data collection (1c). Data Retention subgroup should work in concert with Collection group on best practices regarding what information qualifies as PI, and does the collection and merging of multiple bits of non-PI data result in a "profile" that requires the same best practices as PI?
    c. **Security.** Determine what are industry standards for data security – is the size of the database a determining factor for the level of security? Should it be based on the sensitivity of the information (i.e., HIPPA and Financial Privacy regulations)? What are reporting standards in case of data breach? Are there best practices that can overcome the current patchwork of state and international regulations?
    d. **Access and Accuracy.** How does industry deal with correction of data in the context of third party sharing; what is the responsibility of the original collector to provide access and accuracy tools? Does access and accuracy responsibility lie solely with the holder of the data (i.e. if information is collected by a mobile app but never retained, is the app developer still responsible for accuracy of the data if it now resides with a large data broker)?

3. Data Sharing Working Group
    a. **Individual Control.** Establishment of clear, effective notification language; how does "just in time" notification function when data may not be shared immediately. How do we notify users when data is being shared with third

parties at the time of collection, while still adhering to Human Interface Guidelines and best practices of user interface design.

b. **Transparency.** in the context of data sharing, transparency and control should be topics taken together, rather than as two separate working groups.
c. **Context.** As in the data collection working group, clear definitions of PI must be established, and agreed to practices regarding the sharing of data that is PI. Additionally, the subgroup may consider consumer education regarding the sharing of public data, which should not be considered PI but may have overall implications for consumer comfort on the Internet.
d. **Access and Accuracy.** Establishment of best practices regarding who holds responsibility to update data, and, in conjunction with working groups dealing with context, when a company or non-profit (like opensecrets.org) is responsible for the correction of data, including publicly available data sourced from government agencies.

Note on Accountability:

> All three areas have roughly the same requirements under "Accountability". While we believe strongly in the industry's ability to implement self-regulatory measures, it is clear that bad actors deserve swift enforcement response. When reckless companies get attention for violating consumers' privacy rights it's bad for everyone's business. Developers only enjoy success in the marketplace when consumers have confidence in the safety of their personal information online.

We believe the above framework presents a starting point for the workgroups that does not limit the focus to a specific technology or collection device, but instead allows them to address the core issues surrounding the data itself. This will allow key stakeholders from all points along the data collection and usage path to be part of, and responsible for, its success.

Concerns Regarding Transparency

While we are thankful to be part of the multi-stakeholder proceedings and believe it is critical that app developers have a role in these discussions, we have a few concerns about the transparency process initiated by the NTIA. Obviously, we value transparency and benefit from it daily in how we conduct business within the United States. However, it is crucial for participants in this process to feel unfettered in their participation, free to

engage in wide-ranging discussion and propose bold solutions. We believe the free exchange of ideas is likely be sharply curtailed by the format of the discussions.

Columnist and interviewer Fareed Zacharia noted at a public speech celebrating the twenty-fifth anniversary of the first ".com" on the Internet that "too much transparency could actually stifle democracy". He noted that if every comment made is broadcast, then the instinct of politicians (and we believe business leaders) is to focus on only appealing to supporters, rather than engaging others as equals.

If this stakeholder process takes the form of a public discussion, industry participants will be looking over their shoulders or sitting on their hands instead of offering bold ideas for workable solutions. Fully transparent proceedings will not produce the free exchange of ideas and consensus agreement that is the stated aim of the stakeholder process. For NTIA to get the best results from these efforts, they need to value positive outcomes more than an open process.

We believe the multi-stakeholder process should be transparent when full meetings are taking place, but that NTIA officials be able to meet with subgroups and serve as a sounding board to ideas prior to their being included in larger meetings.

Strong guidance on implementation can be found from the alternative dispute resolution (ADR) community. The U.S. Office of Personnel Management has considerable resources on ADR, and ACT is happy to work with NTIA staff on implementation[9].

App Developers and Industry Groups Taking the Lead on Privacy

Finally, the Request for Comment asks questions about current activities taking place within the industry. While we cannot speak to activities by other groups, we can highlight what the mobile apps community is doing right now to deal with the issues raised in the NTIA paper.

The biggest hurdle to implementing industry-wide privacy standards is developer education. There are over 200,000 app developers in the United States. App makers want to do the right thing on privacy, but often don't know whether their app creates privacy concerns or what they need to do to be rules compliant. As most small business app developers are making customer-facing software for the first time, they are also addressing privacy issues for the first time. Matters typically handled by a legal department or chief privacy officer in a larger company are now most often handled by a small business owner.

[9] http://www.opm.gov/er/adrguide/toc.asp

Recognizing the need to boost developer education, ACT has been particularly active on this issue during the past twelve months. In addition to frequent meetings with lawmakers and regulators here in Washington, we have traveled around the country to speak at developer conferences to raise awareness about consumer privacy.[10] While warning developers about possible new regulations, we have also helped to map out proactive steps they can take.

First and foremost, we advise app developers to be open with consumers about the information they collect and how it is used. We strongly advocate the use of privacy policies – even if an app maker believes no information is being collected. It is also important that this information is presented to users in a meaningful way so that they may easily comprehend it. On mobile devices this means that the information provided must be simple and clear enough to fit on a small screen.

ACT also advises app developers to be mindful of the relationships they have with third parties such as ad networks. App makers must be aware that the software development kits (SDKs) supplied by platform providers or ad networks may contain code that uses consumer information in ways they hadn't considered. Even if the developer never sees the data which passes straight through to an advertiser, the responsibility still lies with the app maker to inform the user what information is shared and how it is being used. Additionally, developers should ensure that they collect only as much information as is needed. When this information is no longer required, it should be de-identified.

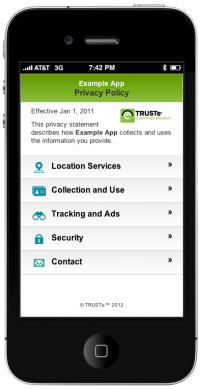
ACT is committed to creating self-regulatory methods to address this problem and we work with developer groups dedicated to finding their own solutions. One such affiliate group is Moms with Apps, comprised of more than one thousand children's app makers. These developers are parents who decided to make apps to educate their children. They are conscious of privacy concerns and the collection of data because the last thing any of them want is to expose their own children's private information.

Moms With Apps Privacy Icon

[10] http://vimeo.com/34560160

Because of this concern, independent developers in Moms with Apps took the initiative to design a parental notification system that identifies the privacy settings of an app in a simple, easy to identify graphical display. While this isn't a final solution, it's a great step initiated from within the industry to safeguard user privacy.

In addition to the initiative shown by these app-making parents, other efforts have also been undertaken by industry to provide improved consumer access to privacy information. To address the accessibility of privacy policies, groups like TRUSTe[11] and PrivacyChoice.org[12] have begun offering privacy policy generators. Developers simply fill out a survey explaining the functions of their app and a privacy policy is automatically generated. This is a useful option for startups that can't afford legal staff. The resulting privacy policy is generated in both the long form that we are accustomed to seeing (and seldom reading) as well as a more easily digestible version composed of simplified language. The other benefit of these services is that they customize the end product to appear on a small screen.



Finally, ACT is moving to address NTIA's questions regarding the issues of small screensize that are particular to our industry. On April 20th 2012, ACT is convening a workgroup on developing privacy notifications for small screen at MoDevUX, the largest single mobile user interface design conference in the world. With more than 500 developers, we believe this industry session and working group will produce tangible products to be reviewed by our larger NTIA-led multi-stakeholder group

NTIA has initiated an ambitious project to address consumer privacy concerns across a wide range of communications platforms. It is faced with an evolving technological landscape that makes this task particularly challenging. ACT believes the only possible way to effectively achieve these goals is through a comprehensive approach to privacy that focuses the data rather than technology.

We look forward to working with our fellow stakeholders and NTIA staff in pursuit of equitable solutions that address what the public really wants: the assurance that their personal information is being treated in a way that matches their expectations.

[11] http://www.truste.com/products-and-services/small_medium_business_privacy/privacy_policy_generator.php
[12] http://www.privacychoice.org/resources/policymaker