Statement of Jonathan Zuck

President

The Association for Competitive Technology

Testimony before the Senate Committee on the Judiciary, Subcommittee on Privacy, Technology, and the Law

"Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones, and Your Privacy"

May 10, 2011

Chairman Franken, Ranking Member Coburn, and distinguished members of the Committee: My name is Jonathan Zuck, and I would like to thank you for holding this important hearing on privacy and the growing mobile devices marketplace.

I am the president of the Association for Competitive Technology (ACT). ACT is an international advocacy and education organization for people who write software programs--referred to as application developers--and providers of information technology (IT) services. We represent over 3,000 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 community leaders are not political spokespersons—they are engineers; and I have drawn upon our membership's technical expertise and business concerns to inspire and inform these comments.

Prior to this hearing, several Senators and their staff asked for information about the size, scope, and impact of this new apps ecosystem; my testimony here strives to answer those questions as well as address concerns on privacy and security regarding mobile devices.

The new mobile apps world has sparked a renaissance in the software industry; small software companies are able to create innovative products and sell them directly to consumers. This is a radical departure from the era of up-front marketing costs, publisher delays, and piracy problems. The mobile app store has eliminated the longstanding barriers to entry that our industry battled for the past two decades.

My goal today is to help explain how small business is building this exciting new industry, how what we are doing is helping consumers, and how the very real concerns about privacy must be dealt with holistically, rather than from a technology-specific perspective.

Finally, for this renaissance to continue, government action must be careful to preserve the opportunities for small businesses to innovate, experiment, and compete with dominant market players.

The Smartphone Ecosystem is Creating Jobs and Opportunities in Tough Economy

The state of the U.S. economy is profoundly unsettled. Questions about job security, healthcare, and foreclosure have become dinner table conversation throughout this country.

In the face of all of this turmoil, there has been a bright spot in economic growth: Sales of smartphones and tablets, such as the iPhone, the HTC Thunderbolt (running Google Android), the Samsung Focus (running Microsoft WP7) , the iPad, Xoom, and now RIM's Playbook, continue to outpace all predictions and are providing a huge growth market in a slumping economy. In fact, nearly one hundred million smartphones were shipped in the first quarter of 2011[1] marking a 79% increase in an already fast growing market.

Vendor	1Q11 Shipments	1Q11 Market Share	1Q10 Shipments	1Q10 Market Share	1Q11/1Q10 Change
Nokia	24.2	24.3%	21.5	38.8%	12.6%
Apple	18.7	18.7%	8.7	15.7%	114.4%
Research In Motion	13.9	14.0%	10.6	19.1%	31.1%
Samsung	10.8	10.8%	2.4	4.3%	350.0%
HTC	8.9	8.9%	2.7	4.9%	229.6%
Others	23.2	23.2%	9.5	17.1%	143.7%
Total	99.6	100.0%	55.4	100.0%	79.7%

Source: IDC Worldwide Quarterly Mobile Phone Tracker, May 5, 2011

Note: Vendor shipments are branded shipments and exclude OEM sales for all vendors. [2]

Smartphones that run third party applications are creating opportunities for handset manufacturers like HTC, Apple, and Motorola, communications firms like Verizon and AT&T, and most especially for application developers like our members.

In 2008, Apple launched an "apps store" to provide a place for developers to sell independently developed applications for the iPhone. Since then, over 300,000 new applications have gone on sale with billions of applications sold or downloaded. The Android platform has recently exceeded the growth rate seen in the iPhone, totaling more than 200,000 applications with 10,000 new programs available each month. In 2010 we saw the release of Windows Phone 7 with its own applications store and an entirely

---

[1] Mark Kurlyandchik, *IDC: Nokia Remains Top Smartphone Vendor Worldwide*, DailyTech, May 6, 2011.
[2] *Id.*

unique user interface. Total unique apps across all platforms are expected to exceed 500,000 by the end of 2011.[3]
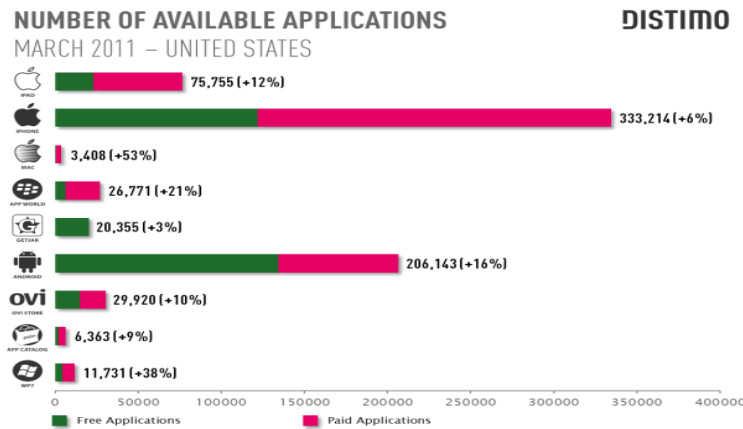

Possibly the most important thing we have noticed about the new apps world is how it has revolutionized the software development industry. It is nothing less than a rebirth. Startup costs of the modern app developer are a fraction of what they used to be just 10 years ago. Gone now are the costs of printing discs, manuals, marketing materials, contracts with retailers, onerous contracts with publishers, and contracts with credit card providers all once necessary to sell a single product. Distribution is now all digital. Those costs savings in distribution are now used to hire more developers and artists, thus creating more jobs across the country. With mobile and Xbox 360 apps, we have seen the return of the small "garage," independent developer focused on products that can be created and shipped in a matter of months. The apps store model creates a direct bridge between the customer and the developer. Our members tell us that being a developer has not been this exciting since the origins of the personal computer and software industry in the 70s and 80s.

So who is this new generation developer? What does an apps creator look like? To find out, ACT conducted surveys and focus groups within our membership and also analyzed the top 500 selling apps.
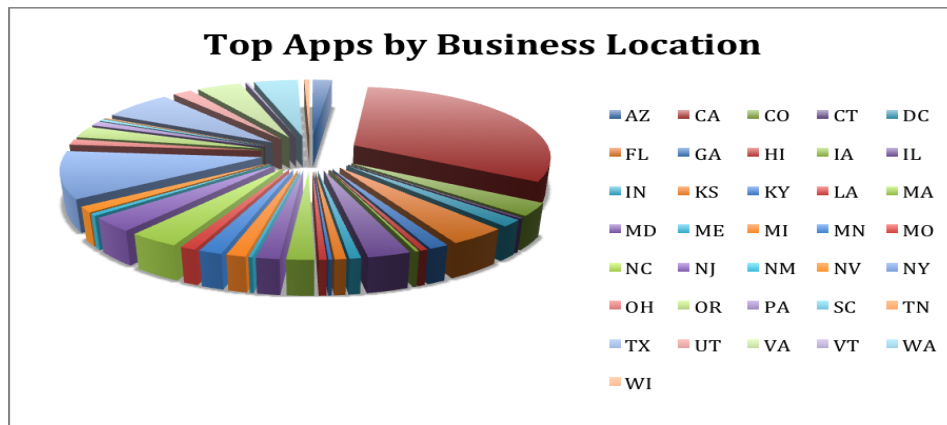
First, we learned mobile apps are overwhelmingly created by developers in small businesses. A review of the top 500 best selling applications show that over 85% are

---

[3] *http://d2omthbq56rzfx.cloudfront.net/wp-content/uploads/2011/04/Distimo-survey-201103-app-stores-count.png*

written by small businesses[4]; in a majority of cases, micro businesses with less than 10 employees.

Top Apps by Business Size

- Small Business (>250)
- Large Business (<250)
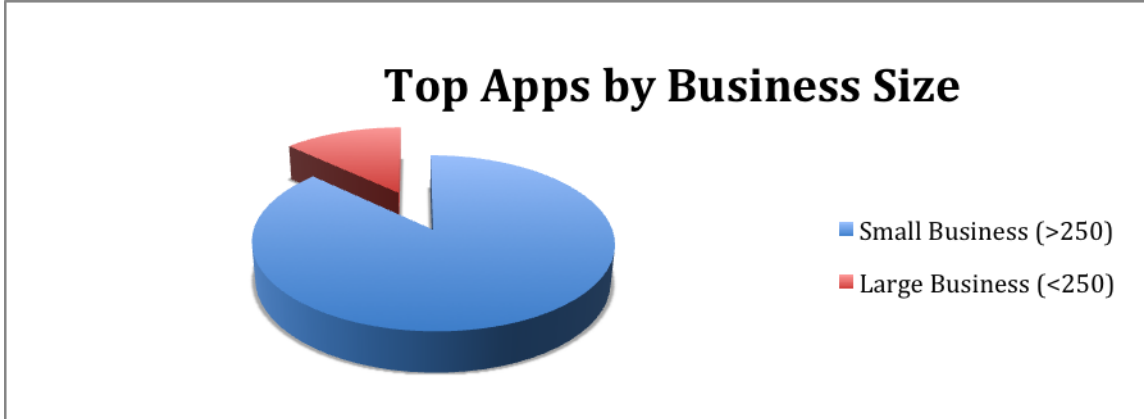
Second, app developers are not just in California. During the dotcom boom of the 1990s, the majority of growth occurred in Silicon Valley while the rest of the country did not reap all of the benefits of the economic boom. Conversely, the recent growth of the mobile apps industry has led to job creation all across the United States. While California continues to have a large representation of apps developers, nearly 70% of the businesses are located outside of the state of California. The independent nature of this burgeoning industry allows developers to live almost anywhere, including Moorhead, MN, and Tulsa, OK[5].

Top Apps by Business Location

- AZ
- CA
- CO
- CT
- DC
- FL
- GA
- HI
- IA
- IL
- IN
- KS
- KY
- LA
- MA
- MD
- ME
- MI
- MN
- MO
- NC
- NJ
- NM
- NV
- NY
- OH
- OR
- PA
- SC
- TN
- TX
- UT
- VA
- VT
- WA
- WI

---

[4] *ACT analysis of top 500 selling apps, some discrepancies exist due to lack of verifiable employment data and apps created by a developer who has significant investment from a larger company. Some apps branded for a larger company are in fact developed by small firms subcontracted to build the application. Sample size of 408 applications, from "top apps" on March 25, 2011.*

[5] *ACT study of top selling apps as of March 25, 2011. ACT members Chalk LLC in Moorhead, MN, and Permafrost Software in Tulsa, OK.*

Third, app development companies have low initial costs, but also have the ability to become a highly successful and sustainable business. ACT's members reported development costs ranging from $1,000 to upwards of $1,000,000. Given the wide range of our findings and those of other reports[6], it is better to view the cost of mobile apps in tiers. In tier one, a simple app with no real back end server based functionality can run in the low thousands; this category makes up a significant percentage of all the apps in various mobile stores. They may be single feature programs, vanity apps, or just irreverent apps like iBeer.

The second tier are the apps that provide multiple levels of functionality. Often working with data stored in a remote server to provide information/user generated content or advanced capabilities like writing and saving specialized documents, this tier runs from $30,000 to $100,000.

The final tier runs from $100,000 on up. This category is for apps that may need to tie into sophisticated inventory management systems, require specialized licenses for content, interface with business critical databases not just to read, but also write information, and finally, games with immersive environments where art and music costs can be significant.

Understanding the Real Opportunity for Small Business

To get a sense of the size of the market and potential opportunity, we must first understand the various business models underlying the mobile app market.   First, there are app developers who charge their customers to download their applications and/or charge them for purchases they make inside the app. For example, photography app Hipstamatic costs $1.99. If users want additional camera effects (Kodachrome or Holga, for instance) they can buy the add-ons in the application.

Second, some apps are supported either entirely or partly by advertising revenue. This is an increasingly important model especially as the Android platform grows in importance. Some applications charge for downloads and run advertisements inside the app itself.

---

[6] *http://appmuse.com/appmusing/how-much-does-it-cost-to-develop-a-mobile-app/*

Finally, many applications are given away free by larger companies in order to extend services to mobile devices or as marketing tools. From Citibank's online banking app to Pepsi's "Refresh Project" and Conde Nast's magazine apps, Fortune 1000 companies are increasingly offering mobile apps to their customers and potential customers. While large companies brand these apps, smaller companies with the expertise necessary to build world-class applications under tight deadlines usually build them.

Mobile App Stores

The exponential growth in app stores during the past few years is unprecedented. Apple launched the mobile app store arena with the iTunes App Store less than 4 years ago, soon followed by Nokia, Google, Microsoft, Amazon, and others. According to IHS, the worldwide market revenue of these app stores in 2010 was $2.15 billion, a 160% increase over 2009, and is expected to reach nearly $4 billion this year. Forrester Research estimates that the revenue created from customers buying and downloading apps to smartphones and tablets will reach $38 billion by 2015.

A growing percentage of revenues for app markets are coming from "in app purchases." According to Xyologic a company that indexes and analyzes app store data, 40 percent of game downloads are now free titles with in-app purchases. In March, it found there were more than 99.9 million downloads of free iPhone games from the App Store.

Yet revenues from app purchases and in-app purchases only represent a part of the overall opportunity for app developers. According to Xyologic, 80.8 percent of all app downloads in the month of March were free. While some of those apps relied on in-app purchasing for revenue, many others were supported by advertising or developed to support other brands and services.

Custom Mobile Development

The majority of the more than 600,000 free apps available across all app stores are not designed to be profitable on their own. They are designed as an extension to an existing service or a marketing program for an established or growing brand. Yet, the value of

these apps and the jobs they create are completely missed by the revenue numbers of app stores and advertising platforms.

This translates into an tremendous number of job-creating opportunities for smaller app development shops. Forrester Research predicts this market to reach $17 billion by 2015.

Mobile Advertising Revenues

In-app mobile advertising is growing more slowly than revenues from app downloads and in-app purchases, but it is a particularly important revenue model for apps with enormous scale, or "eyeballs," like the hugely successful Angry Birds. In the games category, which represents around half the app market, the total revenue from in-app advertising was $87 million according to Juniper Research. Juniper expects that to grow to around $900 million by 2015.

It is also worth noting that the business model of the platform makes a difference in how developers pursue revenue. As shown in an earlier chart, the iOS store has more than 333,000 applications and nearly 70% of those are paid for up front. Google/Android, a company whose entire revenue stream and dominant market position is dependent on advertising, tends to push developers towards the advertising model, with only 30% of the 206,000 apps relying on direct payment to the developer.

The Future for Mobile App Developers

Even more important are the opportunities that lay farther ahead. Members of Congress all have BlackBerries and many have iPhones, Androids, or Windows Mobile devices as well. Yet, according to a recent Morgan Stanley report[7], most people haven't yet invested in such technology. True "smartphones" have around 25% penetration in the U.S.; in Asia, it may be as low as 6%. This represents a pathway for growth leading far into the future.

To understand just how important international sales are to the mobile apps market, one only needs to look at a comparison between the total number of users possessed by a

---

[7]*http://www.morganstanley.com/institutional/techresearch/pdfs/2SETUP_12142009_RI.pdf*

combined AT&T / T-mobile (130 million wireless subscribers)[8] and China's number one wireless carrier, China mobile (584 million subscribers)[9]. Even if only 6% of China's mobile subscribers become smartphone users – and app purchasers – the market opportunity for U.S. software developers is huge.

How Location Based Information Helps Consumers

In the lead up to today's hearing, considerable attention has been directed at the type of information stored on smartphones. A misunderstood element in the public debate on this data collection is the essential role location information plays in the basic function of the device. People buy smartphones to have access to the Internet while they are mobile and a persistent connectivity is essential for this service.

When a smartphone tracks the location of its user, it is making a note to remind itself which access point or cell tower was used there to connect to the Internet. When a user returns to that area, the phone remembers this information. Each day most phone users travel the same route to work or to attend school and then return home to the same place. Keeping this data enables the smartphone to easily find an Internet connection providing efficient, constant online access. This is important for two reasons.

First is battery life. A phone uses a lot of power to search for a cell tower or wireless router. If it constantly needs to search for an Internet connection, it will deplete its battery many times more quickly than if it maintained a constant connection. Customers rate the importance of battery life very highly as a feature in the customer experience, so keeping a charge is a very important requirement of the phone. By maintaining a list of frequently visited locations, a smartphone avoids draining its battery in search of data connection points.

The other reason efficient connectivity matters is spectrum scarcity. The proliferation of smartphones has led to a crowded wireless spectrum, leading to potentially diminishing service quality. Wherever possible, wireless carriers are eager to connect users to wi-fi instead of their networks to provide faster connection speed and to lessen the burden on
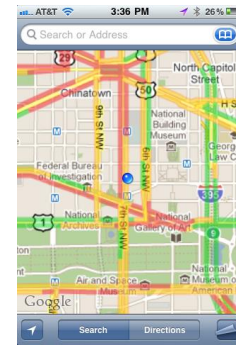
---

[8] *http://www.siouxcityjournal.com/business/local/article_f24b5818-ea11-5f04-b0b0-d7bbd02055b0.html*

[9] *http://www.wirelessweek.com/News/2011/01/Carriers-Subs-Reach-842M-China-Mobile/*

wireless networks. Carriers even provide their own wi-fi service for free to customers in densely populated areas to help alleviate the demand for wireless spectrum. By keeping track of the wi-fi and cell tower locations at frequently visited areas, the smartphone can allow users to automatically switch to wi-fi networks to provide constant, high quality Internet connectivity while diminishing the pressures on a crowded spectrum.

While location data is essential for phones to operate efficiently, consumers also love the smartphone services made possible using location-based technology. Many of the most successful apps or smartphone features have become popular based on knowing exactly where users are at any given time. And that's exactly how customers want it.

Map with Location and Traffic Data

Anyone who has owned a smartphone has probably charted their location as a blue dot on their map app. Many also use those same programs to see where the traffic bottlenecks are before starting their evening commute. Some apps use location to help users find
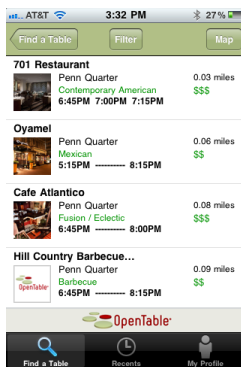
Open Table Reservations

the nearest gas station, post office, parking garage, or coffee shop.

The OpenTable app adds location technology to its existing services to allow diners to find open tables at nearby restaurants, read reviews, and make reservations with a simple tap of the button. Using location information, the app can also provide step-by-step directions to the establishment.

Location services on smartphones have also changed the way we interact socially, creating a market for check-in features to tell your friends and family where you are. Facebook has an app with this feature and, within the last decade, has achieved a market valuation approaching $100 billion. Foursquare, an app which exclusively provides check-in services, has been valued at nearly half a billion dollars.

There is clearly big business opportunity in this marketplace. But location-based services and advertising offer a unique opportunity for Main Street businesses as well. Some apps, like RedLaser, allow users to scan the UPC code of a product and, using the smartphone's location data, find several local retailers nearby where it can be purchased.

Meanwhile, a user searching for a particular product or service on their smartphone can receive an ad from a local small business based on their current location data. These ads have the benefit of reaching potential customers at the exact time of a purchasing decision and cost far less than the newspaper circulars or the TV ads that big box stores are able to afford.

Similarly, local small businesses can also level the playing field with the national chain stores and Internet retailers through shopping apps like Groupon. This app serves 38 million North American subscribers who receive daily discounts at local establishments based on their location data.

While improving the core performance of smartphones, location data is also the building block for apps that users find useful and provide small businesses with opportunities to reach new customers. This data also contains information about the user which they may want to keep private so appropriate safeguards must be in place to ensure it is used in a manner with which consumers are comfortable.

The Smartphone ID Conundrum

Recent news stories have focused on the existence of unique identifiers attached to each smartphone. Known as a UDID number for iPhone and Android ID for Android based products, this is a number that serves as a unique token for each device. The Wall Street Journal article "What They Know - Mobile"[10] made special effort to note the transmission of this number by nearly every single application in the market. While

---

[10] *http://blogs.wsj.com/wtk-mobile/*

highlighting the transmission of a "unique identifier" may make for good newsprint, the article unfortunately did not properly explain why developers transmit this number.

In order to help better explain the role this Smart Phone ID (SPID) number plays in the development and maintenance of mobile applications, ACT surveyed developers[11] to find out how they currently used the SPID number. Respondents highlighted three key uses:

- Allows developers to control access to parts of the program without locking the user out completely (i.e., locking achievement levels in games, viewing paid subscriber content);
- Prevents piracy of applications, allows verification of ownership for updates to apps; and
- Allows management of access control for software testing and customer service.

Additionally, developers reported on several benefits to their customers specifically and consumers in general. Most often cited were:

- Working in concert with other stored data, the SPID makes it possible to have applications remember your favorites even when you buy a new phone;
- Helps content providers know when your device is on a wi-fi network instead of 3G - allowing them to send you HD or other high bitrate content; and
- Makes it easier to receive updates without annoying verification procedures.

At first glance, it would seem to make perfect sense to only allow the SPID to be shared with the app maker itself, but not with third parties. However, in today's world, many different companies work together to provide services to customers. For instance, when shipping a product via FedEx, the sender shares considerable personal information about the recipient with the (third party) shipper including contact information and purchased items. Similarly, small businesses rely on cloud computing to give customers a complete service offering in a cost-effective way. For game developers, a company like OpenFeint offers an easy way to keep track of scores and allows game users to interact with each other, saving app makers thousands of dollars in development time and ongoing infrastructure cost. This service needs to be able to tell devices apart.

---

[11] *ACT April 28 questionnaire to members working on at least one mobile platform. Question: How do you currently use UDID/Android ID in your development process?*

Finally, developers felt that the usage restrictions and best practices for SPIDs were well documented, especially on Apple's iOS. As you can see from the documentation for the UIDevice.uniqueIdentifier[12], Apple gives plenty of advice to app makers on how to properly handle this information [emphasis added]:

> A device's unique identifier (sometimes abbreviated as UDID for Unique Device Identifier) **is a hash value composed from various hardware identifiers such as the device serial number**. It is guaranteed to be unique for each device. The UDID is independent of the device name. For devices that use a SIM (subscriber identity module) card, the UDID is independent of the SIM card.

> For user security and privacy, **you must not publicly associate** a device's unique identifier with a user account.

> You may use the UDID, in conjunction with an application-specific user ID, for identifying application-specific data on your server. For example, you could use a device-user combination ID to control access to registered products or when storing high scores for a game in a central server. However, if you are developing a game, you may want to instead use Game Center's player identifier key as explained in Game Kit Programming Guide.

> Important: **Never store user information based solely on the UDID**. Always use a combination of UDID and application-specific user ID. A combined ID ensures **that if a user passes a device on to another user, the new user will not have access to the original user's data**.

The key takeaway from this survey is that it is important, and often necessary, to keep devices separate and uniquely identified. Users may own many devices, multiple people may share devices (for example, family members), and others switch devices. Developers have different technical reasons to identify devices, but all come down to the same thing: enhancing the user experience. The developer's focus is in making the user's phone more convenient and useful.

While there may be some sinister ways in which the SPID can be illegally used, 99.9% of developers have the very best intentions. Specific instances of SPID abuse should be the focus of FTC action, not the very existence of such a valuable and valid tool.

---

[12] *http://developer.apple.com/library/ios/#documentation/uikit/reference/UIDevice_Class/Reference/UIDevice.html*

Understanding the Existing Laws and Regulations

Regardless of how data protection is approached, it is critical to understand the protections available under existing federal and state laws and regulations. Consumer protection laws with technology-neutral legal standards can address data-privacy and data-security concerns regardless of whether they arise from undisclosed hacking, phishing, lost laptops, website data-collection, inadvertent peer-to-peer "sharing" of sensitive personal files, unauthorized wi-fi-snooping, recklessly designed social-networking applications like Google Buzz, art contests seemingly designed to enable the reverse-engineering of children's social-security numbers, or mobile apps.

Currently, the FTC Act gives the FTC broad authority to act against those who misuse data, regardless of the technology used. Specifically, Section 5 of the FTC Act directs the FTC to take action against any business engaging in "deceptive" or "unfair" trade practices.[13]

The FTC's duty to halt deceptive trade practices authorizes the FTC to take law-enforcement action not only when a business violates explicit promises to consumers,[14] such as violations of stated privacy policies or terms of use, but also even when a business makes material omissions to consumers,[15] such as not telling consumers about the sharing of their collected information with third parties.

Similarly, the FTC's duty to halt unfair trade practices authorizes the FTC to take law-enforcement action when business practices cause injuries to consumers that are: substantial; not outweighed by countervailing benefits to consumers and competition; and could not have been reasonably avoided by consumers themselves.[16] For example, the FTC can take action against a business's failure to report a data breach.

Finally, it is critical to understand two points about consumer-protection laws. First, the FTC has real teeth if it finds that a company engaged in "unfair or deceptive practices,"

---

[13] 15 U.S.C. § 45

[14] *Id.*

[15] FTC, *Policy Statement on Deception (*Oct. 14, 1983) *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

[16] 15 U.S.C. §45(n); *see also* FTC, *Policy Statement on Unfairness* (Dec. 17, 1980) *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

including assessing injunctive and civil penalties. Second, state consumer-protection acts grant state Attorneys General even broader substantive and remedial powers than those that federal law grants to the FTC. As a result, even were resource constraints or agency capture to preclude FTC action in a particular case, 50+ law-enforcement agencies would still have broad, technology-neutral authority to protect the privacy and security of consumers' data.

Consequently, the consumer-protection authority of the FTC and the State Attorneys General already authorizes and requires these law-enforcement agencies to patrol the Internet for companies that might violate their promises to consumers or cause them substantial harm. The FTC recently used such authority to protect consumer privacy by taking action against Google[17] and Chitika[18] for failing to properly handle consumers' information. Both companies now face twenty years of oversight and damage to their brands.

Existing consumer-protection laws thus already authorize both the FTC and state law enforcement agencies to police the entire range of products that connect to the Internet, including mobile devices, and to take action against the bad actors that ignore existing laws and will continue to ignore any future laws. This existing authority also ensures that good actors already have every incentive to behave reasonably and that bad actors have good reason to fear the existing legal consequences of their wrongdoing.

Given the existing authority of the FTC and the State Attorneys General, do we need additional regulation? ACT believes this is an open question, but one where consumer privacy protection should not be viewed through a limited, technology-specific lens. Instead, thoughtful, arduous, and considered discussion must take place on the role of personal data in the economy, the true interests of consumers, and the best interaction between citizens and the providers of products and services that use their data.

---

[17] *In the Matter of* Google Inc., a corporation, FTC File No. 102 3136.
[18] *In the Matter of* Chitika, Inc., a corporation, FTC File No. 1023087.

Avoiding the Patchwork Problem; Dealing with Data Holistically

In periods of great technological change, both new opportunities and new challenges are created. More often than not, however, the seemingly new challenges are merely old issues illuminated under a new light.

Like the dot-com boom before it, the emergence of smartphones and mobile apps has renewed interest in the way corporations and governments collect and share data, most importantly, personal data. Yet, in both cases, these new technologies are simply bringing new light to issues surrounding personal data collection and use that have existed for decades.

There are genuine questions to be asked and considered with respect to the collection and use of personal data. How and when should people be told the data is being collected or when it is being shared? How should they be told? Should people be able to modify data that is collected about themselves? Should people be able to delete data about themselves or otherwise control how it is used? Asking these questions only in the context of smartphones and mobile apps ignores the larger picture. The technology used to collect the data is much less significant than the important questions about the process and behavior of those collecting it.

First, the data collected by apps developers is an almost infinitesimal piece of the global collection of personal data. From credit card companies, to warranty cards, to loyalty programs, companies have been collecting data on their customers long before the Internet or smartphones came around. Not only do other companies collect the same data as smartphone apps, but they have exponentially larger collections of personal data already at their disposal. Information brokers like Epsilon and Google collect, retain, and share far more information than all mobile apps combined.

Even the collection of location data that has been singled out in recent press reports is not unique to smartphones and mobile apps. Standalone commercial GPS providers like TomTom or GPS-based safety services like OnStar collect this information on their users. Your EZ Pass technology for wireless payment of highway tolls also collects and stores location data.   More recently, Google has been collecting personal information while

mapping home and business wireless networks. In nearly every instance, these companies may share that data with third parties.

All of this reminds us that isolating and regulating one specific technology is not the answer to the broader questions surrounding the collection and sharing of personal data. Given the enormity of existing data collections and the number of ways it is amassed, focusing exclusively on one technology – particularly the newest and least established – is a symbolic gesture that does not solve the underlying problem, but creates the false sense that the problem has been solved and the need for thoughtful debate and policy consideration is over. However, focusing instead on regulations of behavior and data usage, it then applies to everyone, regardless of means of collection and sharing.

Finally, perhaps the most dangerous problem is that when regulation focuses solely on new technology, it discriminates against small businesses. Whenever we are talking about new, disruptive technologies, we are most often talking about small businesses. Revenue models, customer expectations, and efficiency opportunities are all still emerging, and it is small businesses that perform that service. Lots of businesses start, a very small number survive, but in the end, we know what works, and then the large businesses get involved. To stunt the growth of a new, experimental market is to discriminate against the very small businesses on which we rely to lead innovation and growth in the American economy.

Conclusion

The future of the digital marketplace looks bright for small business, so long as the marketplace remains dynamic and competitive. This is a more than $10 billion opportunity for small business across the United States. Barriers to entry in the marketplace are currently low, and our members are very excited about the future – according to ACT's Board President, Mike Sax, "Programming is fun again!"

While there are important questions that need to be discussed on personal data collection, retention, and sharing, limiting this question solely to smartphones and mobile apps would be ineffectual and counterproductive.

The use of location information and smartphone ID's are providing immense value to consumers. Whether it's the ability to make dinner reservations or find directions to the nearest hardware store, our members put a value on creating a product that improves the lives of their customers.

Banning the collection of location data would essentially outlaw these beloved consumer apps while doing nothing to address the big questions about data collection and how that data is used. That is why ACT believes that Congress must take a holistic approach to privacy that does not single out any one technology, especially nascent ones. We need to outlaw bad behavior, not good technology. I hope that the committee will continue to focus the spotlight on the contribution small business makes to the future of the digital economy and the way government can do a better job to encourage that productive future. Thank you for your time and consideration on this important topic.