Session 7: New Products, Product Design and the Law

We will look at choices that firms make in designing their products with the law in mind. These choices can raise local, national and international issues. We will look at materials o four different situations: (1) the Federal Trade Commission's July 10, 2014 complaint against Amazon regarding the design of its in-app purchase mechanism on devices like the Amazon Fire tablet; (2) the May, 2014 rideshare ordinance passed by the Chicago City council; (3) the regulatory response to Airbnb and (4) decisions by Apple and Google to boost encryption in their smartphone operating systems and the response of the head of the Federal Bureau of Investigation.

DAVID C. SHONKA
Acting General Counsel
JASON M. ADLER
DUANE C. POZZA
jadler@ftc.gov, dpozza@ftc.gov
Federal Trade Commission
600 Pennsylvania Avenue N.W., CC-10232
Washington, DC 20580
P: (202) 326-3231, (202) 326-2042
F: (202) 326-3239

Local Counsel
LAURA M. SOLIS, WA Bar No. 36005
lsolis@ftc.gov
Federal Trade Commission
915 2nd Avenue, Suite 2896
Seattle, WA 98174
P: (206) 220-4544
F: (206) 220-6366

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

AMAZON.COM, INC.,

Defendant.

Case No. _____

COMPLAINT FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF

Plaintiff, the Federal Trade Commission ("FTC"), for its Complaint alleges:

1. The FTC brings this action under Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), to obtain preliminary and permanent injunctive relief, rescission or reformation of contracts, restitution, the refund of monies paid, disgorgement of ill-gotten monies, and other equitable relief for Defendant's acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), in connection with Defendant's billing for charges related to activity within software applications ("apps") consumers download to their mobile devices from Defendant's app store.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345, and 15 U.S.C. §§ 45(a) and 53(b).

3. Venue is proper in this district under 28 U.S.C. § 1391(b)(1), (b)(2), (c)(2), and (d), and 15 U.S.C. § 53(b).

PLAINTIFF

4. The FTC is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41-58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce.

5. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act and to secure such equitable relief as may be appropriate in each case, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies. 15 U.S.C. § 53(b).

DEFENDANT

6. Defendant Amazon.com, Inc. ("Amazon") is a Delaware corporation with its principal place of business in Seattle, Washington. Amazon transacts or has transacted business in this district and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, Amazon has advertised, marketed, promoted, distributed, offered

for sale, or sold apps that can be downloaded from Amazon's Appstore and installed on its Kindle Fire and Kindle Fire HD devices ("Kindle Fires"), or on mobile devices running the Android operating system ("Android mobile devices").

COMMERCE

7. At all times material to this Complaint, Amazon has maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANT'S BUSINESS PRACTICES

8. Amazon offers thousands of apps through its mobile app store, including games that children are likely to play. In many instances, after installation, children can obtain virtual items within a game, many of which cost real money. Amazon bills charges for items that cost money within the app—"in-app charges"—to the parent. Amazon began billing for in-app charges in November 2011, well after media reports about children incurring unauthorized charges in similar apps from other mobile app stores. Amazon nonetheless often has failed to obtain parents' or other account holders' informed consent to in-app charges incurred by children. Just weeks after Amazon began billing for in-app charges, consumer complaints about unauthorized charges by children on Amazon's mobile devices reached levels an Amazon Appstore manager described as "near house on fire[.]" In total, parents and other Amazon account holders have suffered significant monetary injury, with thousands of consumers complaining about unauthorized in-app charges by their children, and many consumers reporting up to hundreds of dollars in such charges.

Background on Amazon's Appstore

9. Amazon offers apps through its Appstore, a digital store preloaded on Kindle Fires and available for installation on Android mobile devices. Apps provide a wide variety of mobile computing functionality, allowing users to, for example, watch television shows, check the weather, or play games.

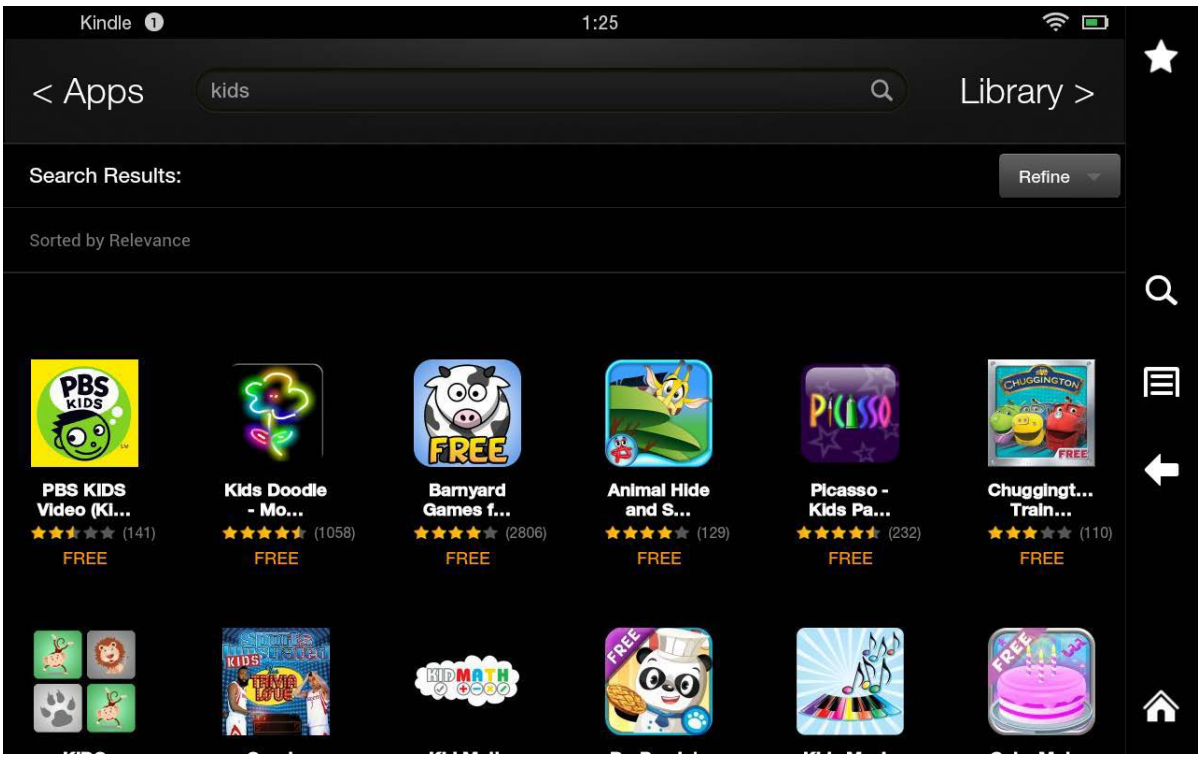
10. Before it agrees to offer any app designed by a third-party developer in the Appstore, Amazon reviews the app's functionality, content, and user experience. Amazon generally assigns each app it sells to at least one topical category, such as "Games" or "News & Magazines." Certain categories expand into subcategories. The "Games" category, for instance, includes subcategories like "Kids" and "Strategy." Amazon also groups apps by price, including the top "Free" apps and top "Paid" apps.

11. Amazon offers apps for free or a specific dollar amount. Amazon also charges account holders for certain user activities within some apps. These in-app charges generally range from $0.99 to $99.99 and can be incurred in unlimited amounts. In many instances, the apps containing in-app charges are games that children are likely to play.

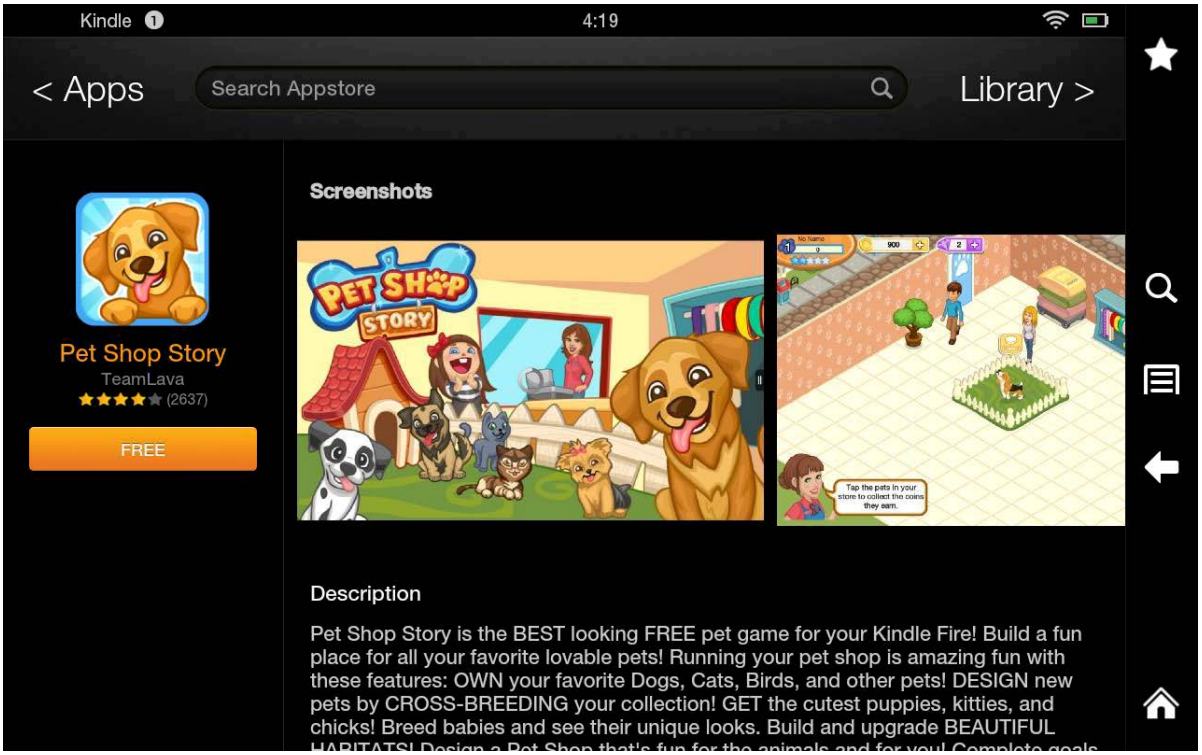
12. Amazon controls the billing process for in-app charges and retains 30% of all revenue from in-app charges, amounting to tens of millions of dollars to date.

Installing an App from Amazon's Appstore

13. Before consumers can install any app, Amazon requires that consumers link their mobile device to an Amazon account funded by a payment method such as a credit card or Amazon.com gift card. To install an app, a parent or other account holder must first locate it by searching for the app by keyword (*e.g.*, the name of the app) or by browsing the various categories and subcategories within the Appstore. In both cases, Amazon displays search results or the contents of a category in rows of app icons accompanied by the name of the app, a user rating, and the price of the app. An example of the results for a keyword search of the word "kids" appears below.



14. By clicking on an app's icon, the account holder can access the app's detail page, such as the one below.



If an account holder scrolls through the detail page, he or she can view the full app description, the app's age rating (*e.g.*, "All Ages"), and other information.

15. Amazon generally appends a note to the end of app descriptions (and often "below the fold," meaning that viewers cannot see it without scrolling down) that mentions in-app charges, but does not explain how or when Amazon seeks account holder authorization for in-app charges. About a year and a half after it began billing in-app charges, Amazon began including a "Key Details" section on the upper right-hand side of the app description that mentions in-app charges, but also does not explain how or when Amazon seeks account holder authorization for in-app charges.

16. On the left-hand side of each app's detail page is a button (the "Price Button") labeled with the price of the app: either "FREE" or a specific dollar amount. To initiate app installation, an account holder must press the Price Button. When pressed, the Price Button changes so that it displays the words "Get App" instead of the price. If pressed again, the app installation process begins.

Incurring In-App Charges

17. After an account holder installs an app, a user can incur in-app charges. In many instances—including in apps that children are likely to play and that are, for example, searchable under the keyword "kids"—these users are children. In many instances, parents have complained that their children could not or did not understand that their activities while playing the app could result in charges that cost real money.

18. When a user engages in an activity associated with an in-app charge (*e.g.*, clicking on a button to acquire virtual treats for use in a game), Amazon displays a popup containing information about the virtual item and the amount of the charge (the "Charge Popup"). A child, however, can clear the Charge Popup simply by pressing a button labeled "Get Item."

19. In many instances, once a user clears the Charge Popup, Amazon does not request any further action before it bills the account holder for the corresponding in-app charge. In these

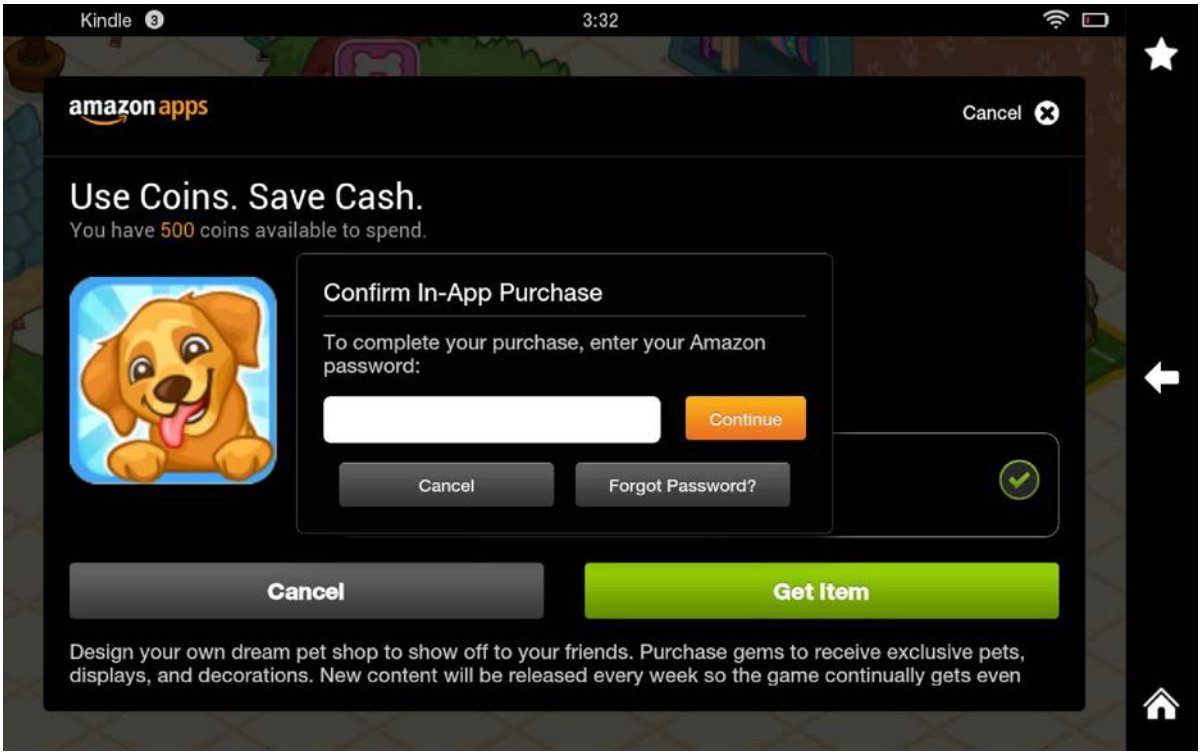
cases, each time a child clears the Charge Popup, Amazon bills the account holder for the in-app charge without requesting his or her consent. Amazon's in-app charge project manager acknowledged this issue the month after Amazon began billing for in-app charges: "[W]e believe that parents are excluded from the buying process for these apps[.]"

20. In or around March 2012, Amazon began requiring password entry to confirm individual in-app charges exceeding $20. In deciding to change its framework for charges above $20, Amazon's Appstore manager noted that "it's much easier to get upset about Amazon letting your child purchase a $99 product without any password protection than a $20 product[.]" An internal document commented that introducing a password prompt for in-app charges over $20 would ensure that those charges were incurred "by the actual accountholder and not someone without permission." Amazon did not implement a password requirement for in-app charges of $20 and under.

21. Not until early 2013 did Amazon adjust its in-app charge framework to require password entry in connection with any other in-app charges. Even then, Amazon's modifications took effect at different times for different device models and, in some instances, have operated in different ways for different apps and different account holders. The password prompts also function differently from the password prompt described in paragraph 20, in that completing the prompt "caches" (that is, stores) the password for a billing window ranging from fifteen minutes to an hour. The net result was that, unbeknownst to many consumers, Amazon sometimes would present account holders with a password prompt to confirm an in-app charge and sometimes would not.

22. Even in those instances in which Amazon has displayed a password prompt, it generally only instructs account holders to enter their Amazon password to "Confirm In-App Purchase" (singular). The prompt in many instances has not provided the amount of the charge or explained that entering a password means Amazon will bill consumers for subsequent in-app

charges over an unspecified duration (ranging from fifteen minutes to an hour) without seeking the account holder's password. A sample password prompt appears below.



23. In many instances, during the processes described in paragraphs 13 to 22, Amazon has not obtained account holders' consent to in-app charges by children.

Amazon Bills Many Parents for Unauthorized In-App Charges Incurred by Children

24. Many of the apps that charge for in-app activities are apps that children are likely to use. Indeed, many such apps are searchable under the keyword "kids," are described or marketed as suitable for children, or are widely used by children.

25. Many of these games invite children to obtain virtual items in contexts that blur the line between what costs virtual currency and what costs real money. The app "Tap Zoo," for example, is a game in which children use "coins" and "stars" to acquire animals, habitats, and staff to populate a virtual zoo. In many instances, the game displays popups with a column containing various quantities of coins or stars. Sometimes, transactions from these popups cost

virtual currency; sometimes, they cost real money. Parents can find the "All Ages" app Tap Zoo by searching the Appstore for the word "kids."

26. Similarly, in the app "Ice Age Village," children manage an ice-age habitat with instructions offered by characters from the animated "Ice Age" movies. The in-game "Shop" offers virtual items, each of which cost a certain amount of virtual currency (either "coins" or "acorns"). The price of each virtual item is displayed on bright green buttons that, when pressed, allow children to purchase the virtual items without any associated real-money charge. But another popup offers coins and acorns with similar bright green buttons that initiate real-money transactions. Children can obtain various quantities of acorns for various amounts of real money, with the largest quantity (2,100) costing $99.99. Parents can find the "All Ages" app Ice Age Village by searching the Appstore for the word "kids."

27. Amazon has received thousands of complaints related to unauthorized in-app charges by children in these and other games, amounting to millions of dollars of charges. In fact, by December 2011, the month after Amazon introduced in-app charges, an Appstore manager commented that "we're clearly causing problems for a large percentage of our customers," describing the situation as "near house on fire." Seven months later, in July 2012, the Appstore manager again described this issue as a "house on fire" situation. Not until June 2014 did Amazon change its in-app charge framework to obtain account holders' informed consent for in-app charges on its newer mobile devices.

28. Many consumers report that they and their children were unaware that in-app activities would result in real monetary loss. For example, one Appstore reviewer complaining about over $80 in unauthorized charges in Tap Zoo commented that her eight-year-old daughter thought she was purchasing the in-game coin packs with virtual currency, not real money. A consumer whose child incurred unauthorized in-app charges in Ice Age Village explained that her daughter "thought she was paying with acorns, but it seems to be hitting my credit card." As one Amazon customer service representative acknowledged in responding to a parent's inquiry

about unauthorized in-app charges: "It's not a hack, but nearly as bad: it's an in-game purchase. A user, such as a child, can easily misinterpret the option to spend actual money as just part of the game."

29. In many games with in-app charges, consumers report that Amazon billed for in-app activities without obtaining their consent. For example, one consumer whose six-year-old "click[ed] a lot of buttons at random (she can't read)" on her Kindle and incurred several unauthorized charges was "shocked that there is no password protection" for in-app charges. Another consumer whose daughters incurred $358.42 in unauthorized charges complained that Amazon allowed the charges without any "step that requires a password to validate payment information."

30. Many children incur unauthorized in-app charges without their parents' knowledge. Even parents who discover the charges and want to request a refund have faced significant hurdles to doing so. Amazon's stated policy is that all in-app charges are final. To the extent consumers have sought an exception to that stated policy, Amazon's process is unclear and confusing, involving emails and web pages that do not explain how to seek a refund for in-app charges, or that suggest that consumers cannot obtain a refund for such charges.

VIOLATIONS OF THE FTC ACT

31. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

32. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers themselves cannot reasonably avoid and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

COUNT I

Unfair Billing of In-App Charges

33. In numerous instances, Defendant has billed parents and other Amazon account holders for children's activities in apps that are likely to be used by children without having obtained the account holders' express informed consent.

34. Defendant's practices as described in paragraph 33 have caused or are likely to cause substantial injury to consumers that consumers themselves cannot reasonably avoid and that is not outweighed by countervailing benefits to consumers or competition.

35. Defendant's practices as described in paragraph 33 therefore constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a) and (n).

CONSUMER INJURY

36. Consumers have suffered and will continue to suffer substantial injury as a result of Defendant's violations of the FTC Act. In addition, Defendant has been unjustly enriched as a result of their unlawful acts or practices. Absent injunctive relief by this Court, Defendant is likely to continue to injure consumers, reap unjust enrichment, and harm the public interest.

37. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC. The Court, in the exercise of its equitable jurisdiction, may award ancillary relief, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law enforced by the FTC.

PRAYER FOR RELIEF

Wherefore, Plaintiff FTC, pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), and the Court's own equitable powers, requests that the Court:

A. Enter a permanent injunction to prevent future violations of the FTC Act by Defendant;

Federal Trade Commission
600 Pennsylvania Avenue N.W.
Washington, DC 20580
(202) 326-2222

B. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendant's violations of the FTC Act, including but not limited to, rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies; and

C. Award Plaintiff the costs of bringing this action, as well as such other and additional relief as the Court may determine to be just and proper.

Dated: July 10, 2014

Respectfully submitted,

DAVID C. SHONKA
Acting General Counsel

s/ Jason M. Adler
JASON M. ADLER
DUANE C. POZZA
jadler@ftc.gov, dpozza@ftc.gov
Federal Trade Commission
600 Pennsylvania Avenue N.W., CC-10232
Washington, DC 20580
P: (202) 326-3231, (202) 326-2042
F: (202) 326-3239

LAURA M. SOLIS, WA Bar No. 36005
lsolis@ftc.gov
Federal Trade Commission
915 2nd Avenue, Suite 2896
Seattle, WA 98174
P: (206) 220-4544
F: (206) 220-6366

OFFICE OF THE MAYOR
CITY OF CHICAGO

FOR IMMEDIATE RELEASE
May 28 2014

CONTACT:
Mayor's Press Office
312.744.3334
press@CityofChicago.org

TRANSPORTATION NETWORK PROVIDERS 'RIDE SHARE' ORDINANCE PASSES CITY COUNCIL
City Establishes Safety Regulations Including First "Surge Pricing" Protections

Mayor Rahm Emanuel announced the City Council today passed the Transportation Network Provider or "rideshare" ordinance that establishes common sense safety regulations for the ride share industry and passengers. The ordinance provides consumer protections, improves passenger safety, meets customer demand while promoting innovation and recognizing the different services and providers throughout our entire public vehicle industry.

"This ordinance will help keep rideshare companies from operating in a regulatory vacuum while increasing public safety, protecting consumers and meeting customer demands for an innovative transportation option," said Mayor Rahm Emanuel. "Residents now have another choice that adds to Chicago's healthy public vehicle industry."

The ordinance requires ride share companies to classify their drivers under the new imposed set of requirements (Class A and Class B) based on the number of hours drivers spend behind the wheel.

- Class A – Companies with company-wide driver averages of 20 hours or less per week logged into the application will need to get City approval of their background check, driver training, vehicle inspection, and zero tolerance drug policies. The license fee will be $10,000. No chauffeur licenses will be required for drivers for Class A companies.

- Class B – Drivers for companies with company-wide driver averages of more than 20 hours a week logged into the application will be required to get public chauffer licenses. The City will conduct the background check and drug test and companies will be required to get an annual 3rd party, 21-point inspection of all vehicles. Like Liveries, vehicles in this class have an age limit of 6 years and must past annual inspections by the City to operate up to 8 years. The companies will need to obtain City approval for their driver training process. License fee is $25,000.

Drivers must meet multiple requirements, including possession of a valid driver's license; a minimum age of 21; no convictions within 12 months of seeking the license of reckless driving, hit and run, more than two moving violations, or license suspension/revocation; no guilty findings

within 5 years for felonies, DUIs, crimes of moral turpitude, and sale or possession of controlled substances.

The City of Chicago is the first city to require surge pricing protections, as prices will be reported before rides are confirmed to ensure the consumer is protected. The ordinance will require companies to publicly announce that such periods are in effect and to take steps to ensure that customers clearly agree to the price, including providing customers with a true fare quote in dollars and cents unless the customer opts out of such a quote. The ordinance also reserves the right to place a cap on surge pricing if the increased disclosure requirements do not alleviate consumer complaints.

The City of Chicago is also the first City in the country to require commercial coverage for the period the driver is logged onto the application and matches state's requirements for personal auto coverage. This ordinance requires $1M in commercial auto liability and in addition, the ordinance also requires commercial general liability insurance with limits of not less than $1,000,000 per occurrence, with the City named as an additional insured party.

"The Department of Business Affairs and Consumer Protection believes this is a balanced approached to regulate public vehicles while providing top notch public chauffeurs," said BACP First Deputy Commissioner Jeffrey Lewelling. "We also look forward to working with the ride share companies in the training, licensing and inspection processes."

This ordinance is packed with benefits for the current taxicab industry. A few examples are it reduces the inspection burden for vehicles younger than 2 years: these vehicles would only have to get an annual inspection, as opposed to a semi-annual one. It increases the incentives for green and wheelchair accessible vehicles by extending the age limits for alternative fuel and WAVs by one year, to 6 years for alternative fuel vehicles and 7 years for WAVs. Liveries are able to provide their own BACP-approved driver training and it establishes a task force to develop recommendations within 60 days for reducing the length of class and increasing convenience for taxi drivers.

In addition, all ride share companies must pay the ground transportation tax and drivers will not be allowed to drive more than 10-hours per day total, and no personal vehicles can be used for more than 10-hours per day for ride sharing.

###

On October 28, 2014, Google officially announced how it would approach encryption in Android 5.0 (also known as lollipop) in a post on its Android blog. And the current statement by Apple on how it manages information requests from the government is here.

James Comey, Director, Federal Bureau of Investigation

Brookings Institution, October 16, 2014

Good morning. It's an honor to be here.

I have been on the job as FBI Director for one year and one month. I like to express my tenure in terms of months, and I joke that I have eight years and 11 months to go, as if I'm incarcerated. But the truth is, I love this job, and I wake up every day excited to be part of the FBI.

Over the past year, I have confirmed what I long believed—that the FBI is filled with amazing people, doing an amazing array of things around the world, and doing them well. I have also confirmed what I have long known: that a commitment to the rule of law and civil liberties is at the core of the FBI. It is the organization's spine.

But we confront serious threats—threats that are changing every day. So I want to make sure I have every lawful tool available to keep you safe from those threats.

An Opportunity to Begin a National Conversation

I wanted to meet with you to talk in a serious way about the impact of emerging technology on public safety. And within that context, I think it's important to talk about the work we do in the FBI, and what we need to do the job you have entrusted us to do.

There are a lot of misconceptions in the public eye about what we in the government collect and the capabilities we have for collecting information.

My job is to explain and clarify where I can with regard to the work of the FBI. But at the same time, I want to get a better handle on your thoughts, because those of us in law enforcement can't do what we need to do without your trust and your support. We have no monopoly on wisdom.

My goal today isn't to tell people what to do. My goal is to urge our fellow citizens to participate in a conversation as a country about where we are, and where we want to be, with respect to the authority of law enforcement.

The Challenge of Going Dark

Technology has forever changed the world we live in. We're online, in one way or another, all day long. Our phones and computers have become reflections of our personalities, our interests, and our identities. They hold much that is important to us.

And with that comes a desire to protect our privacy and our data—you want to share your lives with the people you choose. I sure do. But the FBI has a sworn duty to keep every American safe from crime and terrorism, and technology has become the tool of choice for some very dangerous people.

Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it "Going Dark," and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.

We face two overlapping challenges. The first concerns real-time court-ordered interception of what we call "data in motion," such as phone calls, e-mail, and live chat sessions. The second challenge concerns court-ordered access to data stored on our devices, such as e-mail, text messages, photos, and videos—or what we call "data at rest." And both real-time communication and stored data are increasingly encrypted.

Let's talk about court-ordered interception first, and then we'll talk about challenges posed by different means of encryption.

In the past, conducting electronic surveillance was more straightforward. We identified a target phone being used by a bad guy, with a single carrier. We obtained a court order for a wiretap, and, under the supervision of a judge, we collected the evidence we needed for prosecution.

Today, there are countless providers, countless networks, and countless means of communicating. We have laptops, smartphones, and tablets. We take them to work and to school, from the soccer field to Starbucks, over many networks, using any number of apps. And so do those conspiring to harm us. They use the same devices, the same networks, and the same apps to make plans, to target victims, and to cover up what they're doing. And that makes it tough for us to keep up.

If a suspected criminal is in his car, and he switches from cellular coverage to Wi-Fi, we may be out of luck. If he switches from one app to another, or from cellular voice service to a voice or messaging app, we may lose him. We may not have the capability to quickly switch lawful surveillance between devices, methods, and networks. The bad guys know this; they're taking advantage of it every day.

In the wake of the Snowden disclosures, the prevailing view is that the government is sweeping up all of our communications. That is not true. And unfortunately, the idea that the government has access to all communications at all times has extended—unfairly—to the investigations of law enforcement agencies that obtain individual warrants, approved by judges, to intercept the communications of suspected criminals.

Some believe that the FBI has these phenomenal capabilities to access any information at any time—that we can get what we want, when we want it, by flipping some sort of switch. It may be true in the movies or on TV. It is simply not the case in real life.

It frustrates me, because I want people to understand that law enforcement needs to be able to access communications and information to bring people to justice. We do so pursuant to the rule of law, with clear guidance and strict oversight. But even with lawful authority, we may not be able to access the evidence and the information we need.

Current law governing the interception of communications requires telecommunication carriers and broadband providers to build interception capabilities into their networks for court-ordered surveillance. But that law, the Communications Assistance for Law Enforcement Act, or CALEA, was enacted 20 years ago—a lifetime in the Internet age. And it doesn't cover new means of communication. Thousands of companies provide some form of communication service, and most are not required by statute to provide lawful intercept capabilities to law enforcement.

What this means is that an order from a judge to monitor a suspect's communication may amount to nothing more than a piece of paper. Some companies fail to comply with the court order. Some can't comply, because they have not developed interception capabilities. Other providers want to provide assistance, but they have to build interception capabilities, and that takes time and money.

The issue is whether companies not currently subject to the Communications Assistance for Law Enforcement Act should be required to build lawful intercept capabilities for law enforcement. We aren't seeking to expand our authority to intercept communications. We are struggling to keep up with changing technology and to maintain our ability to actually collect the communications we are authorized to intercept.

And if the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place.

Encryption is nothing new. But the challenge to law enforcement and national security officials is markedly worse, with recent default encryption settings and encrypted devices and networks—all designed to increase security and privacy.

With Apple's new operating system, the information stored on many iPhones and other Apple devices will be encrypted by default. Shortly after Apple's announcement, Google announced plans to follow suit with its Android operating system. This means the companies themselves won't be able to unlock phones, laptops, and tablets to reveal photos, documents, e-mail, and recordings stored within.

Both companies are run by good people, responding to what they perceive is a market demand. But the place they are leading us is one we shouldn't go to without careful thought and debate as a country.

At the outset, Apple says something that is reasonable—that it's not that big a deal. Apple argues, for example, that its users can back-up and store much of their data in "the cloud" and that the FBI can still access that data with lawful authority. But uploading to the cloud doesn't include all of the stored data on a bad guy's phone, which has the potential to create a black hole for law enforcement.

And if the bad guys don't back up their phones routinely, or if they opt out of uploading to the cloud, the data will only be found on the encrypted devices themselves. And it is people most worried about what's on the phone who will be most likely to avoid the cloud and to make sure that law enforcement cannot access incriminating data.

Encryption isn't just a technical feature; it's a marketing pitch. But it will have very serious consequences for law enforcement and national security agencies at all levels. Sophisticated

criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost?

Correcting Misconceptions

Some argue that we will still have access to metadata, which includes telephone records and location information from telecommunications carriers. That is true. But metadata doesn't provide the content of any communication. It's incomplete information, and even this is difficult to access when time is of the essence. I wish we had time in our work, especially when lives are on the line. We usually don't.

There is a misconception that building a lawful intercept solution into a system requires a so-called "back door," one that foreign adversaries and hackers may try to exploit.

But that isn't true. We aren't seeking a back-door approach. We want to use the front door, with clarity and transparency, and with clear guidance provided by law. We are completely comfortable with court orders and legal process—front doors that provide the evidence and information we need to investigate crime and prevent terrorist attacks.

Cyber adversaries will exploit any vulnerability they find. But it makes more sense to address any security risks by developing intercept solutions during the design phase, rather than resorting to a patchwork solution when law enforcement comes knocking after the fact. And with sophisticated encryption, there might be no solution, leaving the government at a dead end—all in the name of privacy and network security.

Another misperception is that we can somehow guess the password or break into the phone with a so-called "brute force" attack. Even a supercomputer would have difficulty with today's high-level encryption, and some devices have a setting whereby the encryption key is erased if someone makes too many attempts to break the password, meaning no one can access that data.

Finally, a reasonable person might also ask, "Can't you just compel the owner of the phone to produce the password?" Likely, no. And even if we could compel them as a legal matter, if we had a child predator in custody, and he could choose to sit quietly through a 30-day contempt sentence for refusing to comply with a court order to produce his password, or he could risk a 30-year sentence for production and distribution of child pornography, which do you think he would choose?

Case Examples

Think about life without your smartphone, without Internet access, without texting or e-mail or the apps you use every day. I'm guessing most of you would feel rather lost and left behind. Kids call this FOMO, or "fear of missing out."

With Going Dark, those of us in law enforcement and public safety have a major fear of missing out—missing out on predators who exploit the most vulnerable among us...missing out on violent criminals who target our communities...missing out on a terrorist cell using social media to recruit, plan, and execute an attack.

Criminals and terrorists would like nothing more than for us to miss out. And the more we as a society rely on these devices, the more important they are to law enforcement and public safety officials. We have seen case after case—from homicides and car crashes to drug trafficking, domestic abuse, and child exploitation—where critical evidence came from smartphones, hard drives, and online communication.

Let's just talk about cases involving the content of phones.

In Louisiana, a known sex offender posed as a teenage girl to entice a 12-year-old boy to sneak out of his house to meet the supposed young girl. This predator, posing as a taxi driver, murdered the young boy and tried to alter and delete evidence on both his and the victim's cell phones to cover up his crime. Both phones were instrumental in showing that the suspect enticed this child into his taxi. He was sentenced to death in April of this year.

In Los Angeles, police investigated the death of a 2-year-old girl from blunt force trauma to her head. There were no witnesses. Text messages stored on her parents' cell phones to one another and to their family members proved the mother caused this young girl's death and that the father knew what was happening and failed to stop it. Text messages stored on these devices also proved that the defendants failed to seek medical attention for hours while their daughter convulsed in her crib. They even went so far as to paint her tiny body with blue paint—to cover her bruises—before calling 911. Confronted with this evidence, both parents pled guilty.

In Kansas City, the DEA investigated a drug trafficking organization tied to heroin distribution, homicides, and robberies. The DEA obtained search warrants for several phones used by the group. Text messages found on the phones outlined the group's distribution chain and tied the group to a supply of lethal heroin that had caused 12 overdoses—and five deaths—including several high school students.

In Sacramento, a young couple and their four dogs were walking down the street at night when a car ran a red light and struck them—killing their four dogs, severing the young man's leg, and leaving the young woman in critical condition. The driver left the scene, and the young man died days later. Using "red light cameras" near the scene of the accident, the California Highway Patrol identified and arrested a suspect and seized his smartphone. GPS data on his phone placed the suspect at the scene of the accident and revealed that he had fled California shortly thereafter. He was convicted of second-degree murder and is serving a sentence of 25 years to life.

The evidence we find also helps exonerate innocent people. In Kansas, data from a cell phone was used to prove the innocence of several teens accused of rape. Without access to this phone, or the ability to recover a deleted video, several innocent young men could have been wrongly convicted.

These are cases in which we had access to the evidence we needed. But we're seeing more and more cases where we believe significant evidence is on that phone or a laptop, but we can't crack the password. If this becomes the norm, I would suggest to you that homicide cases could be stalled, suspects could walk free, and child exploitation might not be discov-

ered or prosecuted. Justice may be denied, because of a locked phone or an encrypted hard drive.

My Thoughts

I'm deeply concerned about this, as both a law enforcement officer and a citizen. I understand some of this thinking in a post-Snowden world, but I believe it is mostly based on a failure to understand why we in law enforcement do what we do and how we do it.

I hope you know that I'm a huge believer in the rule of law. But I also believe that no one in this country should be above or beyond the law. There should be no law-free zone in this country. I like and believe very much that we need to follow the letter of the law to examine the contents of someone's closet or someone's cell phone. But the notion that the marketplace could create something that would prevent that closet from ever being opened, even with a properly obtained court order, makes no sense to me.

I think it's time to ask: Where are we, as a society? Are we no longer a country governed by the rule of law, where no one is above or beyond that law? Are we so mistrustful of government—and of law enforcement—that we are willing to let bad guys walk away…willing to leave victims in search of justice?

There will come a day—and it comes every day in this business—where it will matter a great deal to innocent people that we in law enforcement can't access certain types of data or information, even with legal authorization. We have to have these discussions now.

I believe people should be skeptical of government power. I am. This country was founded by people who were worried about government power—who knew that you cannot trust people in power. So they divided government power among three branches, with checks and balances for each. And they wrote a Bill of Rights to ensure that the "papers and effects" of the people are secure from unreasonable searches.

But the way I see it, the means by which we conduct surveillance through telecommunication carriers and those Internet service providers who have developed lawful intercept solutions is an example of government operating in the way the founders intended—that is, the executive, the legislative, and the judicial branches proposing, enacting, executing, and overseeing legislation, pursuant to the rule of law.

Perhaps it's time to suggest that the post-Snowden pendulum has swung too far in one direction—in a direction of fear and mistrust. It is time to have open and honest debates about liberty and security.

Some have suggested there is a conflict between liberty and security. I disagree. At our best, we in law enforcement, national security, and public safety are looking for security that enhances liberty. When a city posts police officers at a dangerous playground, security has promoted liberty—the freedom to let a child play without fear.

The people of the FBI are sworn to protect both security and liberty. It isn't a question of conflict. We must care deeply about protecting liberty through due process of law, while also safeguarding the citizens we serve—in every investigation.

Where Do We Go from Here?

These are tough issues. And finding the space and time in our busy lives to understand these issues is hard. Intelligent people can and do disagree, and that's the beauty of American life—that smart people can come to the right answer.

I've never been someone who is a scaremonger. But I'm in a dangerous business. So I want to ensure that when we discuss limiting the court-authorized law enforcement tools we use to investigate suspected criminals that we understand what society gains and what we all stand to lose.

We in the FBI will continue to throw every lawful tool we have at this problem, but it's costly. It's inefficient. And it takes time.

We need to fix this problem. It is long past time.

We need assistance and cooperation from companies to comply with lawful court orders, so that criminals around the world cannot seek safe haven for lawless conduct. We need to find common ground. We care about the same things. I said it because I meant it. These companies are run by good people. And we know an adversarial posture won't take any of us very far down the road.

We understand the private sector's need to remain competitive in the global marketplace. And it isn't our intent to stifle innovation or undermine U.S. companies. But we have to find a way to help these companies understand what we need, why we need it, and how they can help, while still protecting privacy rights and providing network security and innovation. We need our private sector partners to take a step back, to pause, and to consider changing course.

We also need a regulatory or legislative fix to create a level playing field, so that all communication service providers are held to the same standard and so that those of us in law enforcement, national security, and public safety can continue to do the job you have entrusted us to do, in the way you would want us to.

Perhaps most importantly, we need to make sure the American public understands the work we do and the means by which we do it.

I really do believe we can get there, with a reasoned and practical approach. And we have to get there together. I don't have the perfect solution. But I think it's important to start the discussion. I'm happy to work with Congress, with our partners in the private sector, with my law enforcement and national security counterparts, and with the people we serve, to find the right answer—to find the balance we need.

Thank you for having me here today.