To: Interested Parties
From: Free & Fair Markets Initiative
Date: September 24, 2018
RE: Senate Commerce Committee Hearing Examining Consumer Privacy Protections

INTRODUCTION

In the wake of the Facebook data harvesting scandal that exposed the personal information of 87 million Americans, there is an urgent and ongoing conversation about the need for technology companies to protect consumer data. In a recent Harris X poll, 84 percent of Americans said technology companies should be legally responsible for the content they carry on their systems, and a majority said that large technology companies should be treated by the federal government the same way as big banks. What's more, 83 percent of Americans said that tougher regulations and penalties are needed.

Facing heightened scrutiny and consumer backlash, several technology companies have acknowledged the gravity of the problem and announced concrete plans to address it. Facebook, for its part, released a 9-step plan to safeguard the social media platform from future election hacking. Twitter updated its privacy policy to be more transparent about how data is shared with businesses and advertisers and give users more control over what data gets shared in the first place. Google launched a free Advanced Protection Program that users can opt into to keep their e-mail and other information safe from hackers and other bad actors.

But tech giant Amazon, one of the world's richest and most powerful companies that stockpiles troves of deeply sensitive consumer data, has been far less forthright about any substantive changes it has made compared to its peer companies. For example, Amazon has yet to provide answers about the alarming role its crowdsourcing gig-economy platform Mechanical Turk played in Facebook's data breach scandal. An investigation revealed that Cambridge Analytica used the little-known Amazon platform as a vehicle to get to Facebook, feeding Mechanical Turk users online surveys that enabled data miners to access their Facebook accounts and the accounts of their Facebook friends. And this is only the start of the many data privacy issues Amazon has failed to address.

During the September 26 Senate Commerce Committee hearings, lawmakers must focus on four critical areas of concern regarding Amazon's data privacy policies and practices:

- **Anti-competitive data hoarding**: Amazon forces its third-party sellers to agree to unlimited use of seller data. Amazon surveils its e-commerce platform for consumer shopping habits and uses that information to steer customers toward its own private label brands and crush third-party sellers; users have a right to know the full extent to which this practice is limiting consumer choice.

- **Data exploitation**: Amazon has plans to cash in on its massive collection of consumer data by expanding its multibillion-dollar advertising business; users deserve to know if their purchase or streaming histories are up for sale.

- **Alexa eavesdropping**: Amazon's smart-speaker has already been caught recording private conversations, and the tech giant has patents pending that could make Alexa even more invasive; those who own an Echo device have a right to know exactly when it is listening.

- **Cloud security**: An unprecedented amount of corporate welfare is subsidizing Amazon data centers in communities across the country and the tech giant is scooping up government cloud contracts left and right; taxpayers deserve to know if their money is funding a secure operation and whether sensitive civic information is being housed on the same servers as consumer information.

The reality is that data privacy threats extend far beyond social media platforms, and the stakes could not be higher when it comes to the threats posed by Amazon. The tech giant knows what we buy online, what we eat, what we watch and soon it might know what medications we take as it tries to upend the health care industry. Single-source cloud contracts from the Pentagon would even make Amazon the custodian of government secrets. The Senate Commerce Committee must use these hearings to ask the many questions on data privacy that Amazon has failed to answer.

I. ANTI-COMPETITIVE DATA HOARDING

Amazon's hybrid e-commerce business model, in which the company acts both as a platform for sellers and a seller itself, is replete with conflicts of interests that ultimately limit consumer choice. For example, Amazon has data on sales trends and consumer behavior that allows it to manipulate prices and drive consumers to its own products and services – which third-party sellers have long voiced concerns about. Practices like these extend far beyond free market competition and raise a critical issue of whether Amazon is improperly using consumer information to stamp out competition.

Questions

The E.U. just launched an investigation to determine if Amazon is using data collected about third-party sellers on its e-commerce platform to gain an unfair advantage, and similar concerns have been raised in the United States as the Federal Trade Commission (FTC) looks into the state of competition and consumer protection. With roughly 1 in every 2 dollars spent online going to Amazon, there is clearly reason to worry, especially for small businesses who sell on the tech giant's platform.

- For a chance to get this on the record, can Amazon say that it categorically does not use data on third-party sellers to gain a competitive edge?

First and foremost, recent reports showed that Amazon employees are unlawfully leaking insider information about sales trends and consumer behavior to select companies.

- How could this possibly happen and what action is Amazon taking to stop this illegal activity in the future? Is the company aware of other illegal activity as it relates to data leaks that the public does not know about?

Amazon provides third-party retailers with consumer information through a program called Amazon Retail Analytics Premium, but the program is unaffordable for many small businesses selling on Amazon's site and even for those that can afford it, Amazon does not release all information – it does not reveal consumer browsing activity. This gives Amazon an unfair advantage since only they can see when a user adds and then deletes something from their cart, for example.

- Does Amazon's brokering of information about consumer behavior e-commerce platform create an uneven playing field for small businesses and independent brands?

It has also been reported that Amazon steers customers away from major brands to their own private-label products with predatory pricing. For example, Amazon ate into roughly one-third of the online battery market within just a few years by underselling Energizer and Duracell with cheap AmazonBasics batteries.

- Can you say with absolute certainty that Amazon does not take data from sellers on the platform and use that to data to inform its Private Label brand decisions? If yes, then why won't Amazon limit its use of third-party seller data accordingly in its seller agreements? Why won't Amazon set up a firewall between its retail and marketplace businesses?

- Sellers have complained about Amazon's seller data use for a long time now, but they also say they feel forced to continue offering products on Amazon's platform because Amazon is a monopoly in third party seller services. What is Amazon's market share in offering marketplace services to third party sellers?

Reporting
EU Starts Preliminary Probe into Amazon's Treatment of Merchants. "EU Competition Commissioner Margrethe Vestager said Wednesday that investigators recently sent out questionnaires to merchants that sell through Amazon. The probe focuses on whether Amazon is gaining a competitive advantage from data it gathers on every transaction and from every merchant on its platform, Ms. Vestager said. "'The question here is about the data,' Ms. Vestager said." (The Wall Street Journal, 9/19/18)

How Amazon Steers Shoppers to Its Own Products. "Around 2009, Amazon quietly entered the private label business by offering a handful of items under a new brand called AmazonBasics. Early offerings were the kinds of unglamorous products that consumers typically bought at their local hardware store: power cords and cables for electronics and, in particular, batteries — with prices roughly 30 percent lower than that of national brands like Energizer and Duracell. The results were stunning. In just a few years, AmazonBasics had grabbed nearly a third of the online market for batteries, outselling both Energizer and Duracell on its site." (The New York Times, 6/23/18)

Amazon Has Access To Sales Data Its Third-Party Sellers Do Not: Shopper's Browsing And Purchase Behavior. "Amazon's third-party marketplace and its millions of sellers across the world have grown into a billion-dollar sales stream for the company since the marketplace first launched in 2000. But as Amazon sells competing products at significantly lower prices and expands its private-label brands, some of the site's third-party sellers say the retail giant is squeezing them out […] Amazon also has an edge when it comes to gathering shopping data on its platform, which national brands and third-party sellers do not have access to, said Thomson. Amazon can track shoppers' browsing and purchase behavior while they click through the site. This gives it access to troves of information about what shoppers are looking for and who to target with more affordable Amazon products. 'If I'm a private-label seller, another private-label seller can come along and create a cheaper version,' said Thomson. 'All those other sellers have profit needs and they're all playing by the same rules. But Amazon has perfect data.'" (Buzzfeed News, 6/13/18)

Amazon Tracks Sales From Third-Party Sellers, Then Uses That Data To Outsell Those Same Sellers. "According to new research from Upstream Commerce, Amazon tracks third-party sales on its site and uses that data to sell the most popular items in direct competition with marketplace members […] Upstream reported that it came across Amazon's activity while conducting a competitive analysis for clients of women's clothing brands on the site. In total, Upstream sampled 857 women's clothing products initially sold by marketplace sellers and checked to see when Amazon initiated selling the same items. Within 12 weeks, Amazon began selling 25 percent of the top items first sold through marketplace vendors." (Forbes, 10/30/14)

II. DATA BROKERING

Introduction

Amazon is on track to be the third-largest digital advertiser in the US, just behind Google and Facebook, and the tech giant is planning on expanding its multibillion-dollar ad business. But unlike Google and Facebook, which give users the option to control what information is shared with third parties, Amazon gives users very limited flexibility regarding privacy – even though the stakes are higher on Amazon, given that users purchase products that can be extremely private.

Questions

Amazon consumers do everything from shopping for food and household products on the website to streaming television shows and movies and reading e-books.

- What kind of data do you collect on consumer behavior, and can you say with complete confidence that protections are in place that would prevent that data from being able to be hacked?

In the wake of the Cambridge Analytica scandal, Facebook publicized a little-known feature on its platform that allows users to download a copy of everything the social media giant knows about them.

- Does Amazon offer an option for users to download a report of everything the company knows about them?

This year, the General Data Protection Regulation (GDPR) went into effect in the UK. The law focuses on consumer consent when it comes to sharing their personal information, and prohibits companies from bundling consent agreements – meaning a single user agreement will not suffice.

- Does Amazon support laws similar to the GDPR for the US, and does Amazon support the "information fiduciary" precedent that says companies must protect consumer data and pledge not to utilize the data for its own benefit, or for the benefit of third-parties?

Reporting

Advertisers Are Flocking To Amazon For The Purchase Insight The Company Provides. "The world's biggest online retailer will generate $4.61 billion in US ad sales this year, which represents 4.2 percent of the total digital ad market, EMarketer Inc. estimated Wednesday in a report […] Amazon is closest to customers at the moment of purchase compared with Google and Facebook, which are better for building brand recognition, EMarketer analyst Monica Peart said. 'Advertisers are looking for a third option that ties purchase data directly to the advertisement,' she said." (Bloomberg, 9/19/18)

Amazon's Advertising Opportunities Inch Forward, Providing User Data Competitors Don't Have. "Amazon, which has already reshaped and dominated the online retail landscape, is quickly gathering momentum in a new, highly profitable arena: online advertising, where it is rapidly emerging as a major competitor to Google and Facebook […] But in the company's most recent financial results, it was a category labeled 'other' that caught the attention of many analysts. It mostly consists of revenue from selling banner, display and keyword search-driven ads known as 'sponsored products.' That category surged by about 130 percent to $2.2 billion in the first quarter, compared with the same period in 2017 […] 'We can reach the right consumer at the right time using their wealth of data to target,' Ms. McGurk said. 'Other traditional digital platforms do not have the level of purchase data that Amazon has on their customers.'" (New York Times, 9/3/18)

Amazon's Ad Revenue Grew 132 percent With Data That's Valuable To Advertisers. "The company's 'other' revenue, which largely comes from advertising, hit $2.2 billion in the second quarter, which was up a whopping 132 percent from the same period last year. This fiscal year, Amazon's other revenue should reach $10.3 billion, accounting for some 8 percent to 10 percent of its total sales, he projects. And that could be only the start of its rapid growth. To Morgan, Amazon has the potential to be the third major player in digital advertising, alongside Google and Facebook. To him, here's what Amazon has going for it: It has data that's valuable to advertisers […] That ability to reach so many consumers along with the data that Amazon has on their shopping habits could make audio ads distributed through Alexa another big opportunity for the company, he said. 'This is something a lot of people don't talk about,' he said, referring to

Amazon's advertising business. ‘It's under the weeds.’ But, he continued, the ad business, could be ‘another gold mine.’” (Business Insider, 8/30/18)

Amazon Beats Competitors For Advertising Dollars Because It Knows Your Intent To Buy. “Amazon is in a unique position to challenge the online advertising duopoly of Facebook and Google because, as Lane writes, ‘Google might know what you’re interested in buying, Facebook might be able to deduce what you’d be inclined to buy, but Amazon knows what you’ve actually bought, or even whether you showed intent to buy.’” (Geekwire, 9/4/18)

III. ALEXA EAVESDROPPING

Despite falling outside of the traditional category of social media, Amazon stockpiles personal data in the cloud just like Facebook does, making it similarly vulnerable to hacks carried out by bad actors. In recent years, the tech giant has gone all-in on the business model of scooping up personal information and using that information to inform its offerings – all while failing to reveal what, exactly, it does with the data. The tech giant’s flagship smart-speaker, Echo – and its automated voice Alexa – provides important and alarming insight into where Amazon intends to go with artificial intelligence and how it sees its users as malleable guinea pigs.

Questions

Amazon allows third-party developers to create their own mini-applications called “skills” that run on Echo and teach the device various methods of picking up voice cues.

- How do you monitor the access you give developers who use your platform and ultimately gain access to user data, and does Amazon have a set of fundamental privacy principles it abides by?

It’s been proven that Alexa software can be modified by third-party developers to eavesdrop – and while Amazon claims to have taken steps to address those vulnerabilities, loopholes like this are still a concern.

- What are you doing on a consistent basis to monitor vulnerabilities on Echo, and have there been any breaches that the public does not know about?

Amazon is branching out with its Alexa-powered devices and recently released several new products, including a microwave oven, an amplifier, a receiver, a subwoofer and an in-car gadget.

- With Echo poised to have an even bigger footprint into the personal daily lives of consumers, what data privacy safeguards are in place to protect the collection of data from these devices?

Reporting

Amazon’s Echo Listened To A Conversation And Then Sent It To An Acquaintance. “The couple got a phone call from an employee of Danielle’s husband. The message: ‘Unplug your

Alexa devices right now. You’re being hacked.’ After the devices were unplugged, the caller told the couple how he received the audio files. ‘At first, my husband was, like, ‘no you didn’t!’ And the (recipient of the message) said ‘You sat there talking about hardwood floors,’’ Danielle told the station. ‘And we said, ‘oh gosh, you really did hear us.’’” (Huffington Post, 5/24/18)

Amazon Admits Its Alexa Device Recorded A Conversation And Then Sent It To An Acquaintance. “Echo woke up due to a word in background conversation sounding like ‘Alexa.’ Then, the subsequent conversation was heard as a ‘send message’ request. At which point, Alexa said out loud ‘To whom?’ At which point, the background conversation was interpreted as a name in the customers contact list. Alexa then asked out loud, ‘[contact name], right?’ Alexa then interpreted background conversation as ‘right’. As unlikely as this string of events is, we are evaluating options to make this case even less likely.” (Recode, 5/24/18)

A Program For The Echo Was Created To Spy On And Record Everything A Person Said. “Security researchers have discovered a vulnerability that enabled Amazon’s voice assistant, Alexa, to listen in on people’s conversations after the ‘Alexa’ wake-up word had been detected […] The researchers created a skill for Alexa, in this case a calculator, that was able to record and transcribe everything a person said and send that data back to a third party.” (Internet of Business, 4/20/18)

Data From The Echo Was Collected And Used By Law Enforcement In A Homicide Investigation. “Perhaps the most famous case of cutting-edge consumer technology being used to gather evidence in a criminal prosecution is the so-called ‘Amazon Echo Murder,’ […] Technology enters the story because a witness who was at Bates's house earlier that night recalled that Bates's Amazon Echo was streaming music. With that piece of information, Benton County, AR, prosecutors sought recordings, transcripts, and other information that may have been captured by Bates’ Echo from Amazon […] Amazon initially opposed authorities' request for the data. But after Bates gave Amazon the go ahead, the company turned over data in April 2016.” (LifeWire, 2/14/18)

IV. CLOUD SECURITY

Having already received over $1.5 billion in taxpayer subsidies since 2000, Amazon is scoring massive government cloud contracts in cities and states are the country. Through Amazon Web Services (AWS), Amazon hosts police department data and electoral data, among countless other kinds of sensitive information. Now Amazon is the favorite to win the JEDI contract. By awarding Amazon contract after contract, lawmakers are essentially taking Amazon’s word that it will take the necessary measures to protect civic data. We cannot afford to simply take Amazon at its word.

Questions

Amazon has repeatedly pointed to user error in the cases of cloud data breeches – and has worked to help educate users and companies about best practices, yet these massive exposures still take place. Just this year, accounts owned by Verizon Wireless, Time Warner and Down Jones & Co., among others, have been compromised.

- Is Amazon responsible for data breeches and exposures on the cloud, and How does Amazon plan to combat future problems with data exposure?

As voter data and activity has proven to be a major area of manipulation for foreign entities, especially in the wake of Facebook's Cambridge Analytica scandal, Amazon CEO Jeff Bezos has said that he sees no correlation between that vulnerability and any possible or perceived vulnerabilities with Amazon. However, massive amounts of voter data are stored on Amazon cloud servers and is vulnerable to these same exposures that have previously happened.

- Is voter information stored on the same servers as consumer information, and can Amazon guarantee the American people that voter information is safe from hacks on the AWS cloud?

Reporting

Amazon's Cloud Storage, Simple Storage Service (S3) Is Notoriously Vulnerable To Many High-Profile Data Exposures. According to recent statistics, as many as 7 percent of all S3 servers are completely publicly accessible without any authentication and 35 percent are unencrypted. [Examples of security breaches:]
Booz Allen Hamilton *When:* May 2017. *Data Exposed:* Battlefield imagery and administrator credentials to sensitive systems. *The Lowdown:* The U.S. defense contractor left data publicly accessible through an insecurely configured S3 account containing files related to the National Geospatial-Intelligence Agency (NGA), which handles battlefield satellite and drone imagery.
U.S. Voter Records *When:* June 2017. *Data Exposed:* Personal data about 198 million American voters. *The Lowdown:* A Republican-party backed big data firm, Deep Root Analytics, put personal information and voter profiling data at risk by storing them on a wide-open S3 server.
Dow Jones & Co *When:* July 2017. *Data Exposed:* Personally identifiable information for 2.2 million people. *The Lowdown:* Wall Street Journal parent company Dow Jones & Co exposed personal information about more than 2 million customers through sloppy S3 configuration.
Pentagon Exposures *When:* 3 leaks found in September and November. *Data Exposed:* Terabytes of information from spying archive, resume for intelligence positions--including security clearance and operations history, credentials and metadata from an intra-agency intelligence sharing platform. *The Lowdown:* The U.S. Department of Defense (DOD) had an embarrassing run of leak announcements last fall that showed a likely systemic disregard for the risk posed by poorly configured Amazon S3 buckets.
Accenture *When:* October 2017. *Data Exposed:* The keys to the kingdom--master access keys for Accenture's account with AWS Key Management system, plaintext customer password databases, and proprietary API data. *The Lowdown:* Arguably one of the most damaging leaks in 2017 from a business risk standpoint, this doozy of an exposure featured at least four S3 buckets set to public containing a massive amount of mission-critical infrastructure data. (Business Insights, 1/24/18)

Call Data Available For Public Download From An Amazon Web Server Included Individual Notes On People Calling In For Mental Health Assistance. "The nonprofit organization that operates Los Angeles County's social services hotline inadvertently exposed personal information that was stored online, according to county officials and a private security firm that discovered the vulnerability. UpGuard, a cybersecurity firm based in Mountain View, Calif., said it notified the county in April that it discovered exposed Social Security numbers, addresses and sensitive notes about calls regarding mental health and abuse […] the information he discovered included names, email addresses and weakly encrypted passwords of users operating the 211 system, potentially opening them to attack. The data also contained […] detailed notes [that] described an elderly woman with dementia who was allegedly being abused by her son. In another, they described a meth addict who said she was suicidal. A third example included details about a woman who suffered from paranoia and was on the verge of being evicted […] He said it was available for public download from an Amazon web server." (LA Times, 5/17/18)

GoDaddy's Web Hosting Configurations For Thousands Of Systems Was Found Exposed On Amazon's AWS. "On June 19th, 2018, an UpGuard Cyber Risk analyst discovered a publicly readable Amazon S3 bucket named *abbottgodaddy*. Inside were several iterations of a spreadsheet, the latest version of which was named "*GDDY_cloud_master_data_1205 (AWS r10).xlsx*, a 17MB Microsoft Excel file with multiple sheets and tens of thousands of rows. The exposed documents include high-level configuration information for tens of thousands of systems and pricing options for running those systems in Amazon AWS, including the discounts offered under different scenarios." (UpGuard, 8/9/18)

Data, Including Audio Recordings, Text Messages And Photos, From A Phone Spyware Company Was Exposed On An Amazon S3 Bucket. "A company that markets cell phone spyware to parents and employers left the data of thousands of its customers—and the information of the people they were monitoring—unprotected online. The data exposed included selfies, text messages, audio recordings, contacts, location, hashed passwords and logins, Facebook messages, among others, according to a security researcher who asked to remain anonymous for fear of legal repercussions […] Last week, the researcher found the data on an Amazon S3 bucket owned by Spyfone, one of many companies that sell software that is designed to intercept text messages, calls, emails, and track locations of a monitored device. (Motherboard, 8/23/18)

CONCLUSION

The Senate Commerce Committee deserves credit for taking such a critical step by inviting executives from some of the most powerful technology companies to answer urgent questions on data privacy. The international conversation that has erupted in the wake of the Facebook data harvesting scandal raises some of the most important issues of our time, and the Committee should be commended for taking productive steps to engage the stakeholders who have the power to fix what is broken when it comes to data privacy. The reality is that time is of the essence as the pace of technological advancement continues to speed up.

But too often the conversation around data privacy is narrowly confined to the challenges posed by social media – a mistake that the Committee must not make. The potential for data abuse and exploitation extends into almost every aspect of our online lives, and Amazon represents the bellwether of a company stockpiling consumer and taxpayer data with hardly any oversight or accountability. Today's hearings mark a vital starting point, but lawmakers must make it a top priority to protect the American people from threats to their privacy and preserve an economy in which data is not used to destroy competition and consumer choice.