TO: NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, DEPARTMENT OF COMMERCE
FROM: TRUSTED FUTURE

RE: PRIVACY, EQUITY, AND CIVIL RIGHTS REQUEST FOR COMMENT

AGENCY/DOCKET NUMBER: DOCKET NO. 230103–0001
DATE: MARCH 6, 2023

INTRODUCTION

Thank you for the opportunity to comment on addressing the critical issues at the intersection of privacy, equity, and civil rights. We are delighted to be able to respond and provide a perspective based on our research and experience.

Trusted Future is a think tank based in Washington, DC that is dedicated to the idea that we need smarter, more pragmatic and informed efforts to raise the level of trust in today's digital ecosystem in order to expand opportunities for tomorrow. Over the past year our organization has conducted a series of surveys to better understand how Americans are using technology today, the challenges that must be overcome, the opportunities they see from a more trusted technology ecosystem, and the steps they'd like to see policymakers and innovators take to improve trust in technology.

Our research underscores the point that Commerce Secretary Gina Raimondo has made that, *"As we move further into what technology is capable of doing, trust becomes so much more important."* As the data we each generate grows by the day, it is now more critical than ever that we ensure that all Americans – regardless of income, geography, or circumstance – are able to protect the privacy of their data, and benefit from the opportunities that trusted technologies can enable. We therefore welcome this opportunity to share our insights on the important questions that NTIA raises with regards to privacy, equity, and civil rights.

Fundamentally, we believe smart and pragmatic data privacy safeguards can protect you, your loved ones, and your most sensitive information. Whether it's your health data, your family photos, or how you spend your free time, you deserve to be able to protect the privacy of what you read, where you browse, what you buy, and where you go. To do that, privacy should be protected as a basic digital right across the devices you use, the websites you visit, the apps you download, and the places you shop. But too often, our most vulnerable populations bear the brunt of risky or exploitative data practices.

Privacy, equity, and civil rights have now emerged as critical elements for fostering the essential trust that people need to take full advantage of new and emerging technologies.

Given the substantial opportunities emerging over the horizon from continued technological advancements, as a society we need to ensure that the benefits are shared broadly – especially with marginalized and disadvantaged communities that could benefit the most. Enabling broad digital equity and inclusion requires specific efforts to ensure that technologies can be trusted by everyone, because a lack of trust can impede adoption and create new forms of detrimental digital adoption gaps.

For a number of reasons, mobile and connected technologies, and the very sensitive data they generate, store, and protect, is an especially important place to focus. As their ubiquity has grown, the smartphone has increasingly become the primary means by which people are accessing the digital world – and an important enabler of digital equity. As Pew Research points out, while Black and Hispanic adults in the United States remain less likely than White adults to say they own a traditional computer or have high-speed internet at home, they are more likely to own a smartphone. In some cities, such as Detroit and Baltimore, nearly 20% of households only have online access via a cellular data plan, according to a Benton Institute analysis of Census data. They also found that over the last couple of years, growth in smartphone ownership is strongly correlated (0.55) with the share of population at or below the 125% poverty level – suggesting that smartphones are a primary digital on-ramp for low-income Americans.

At the same time, access to these technologies have become even more essential to the way we work, learn, find jobs, gain new skills, access health care, bank, and play.   But as we use our connected technologies for more and more parts of our lives, we are also creating more and more data, often more personal data that requires protection.

While our survey research has found that people love their technologies for what they enable people to do, they also want to trust their technology and have concerns that their privacy is not adequately protected. They want bold action from their leaders to better protect their privacy, improve security, and ensure our digital ecosystem is more equitable, inclusive, and trustworthy for all Americans.

Specifically as it relates to data privacy, we found consumers are concerned that companies collect more data than is necessary, and they want more transparency and control over their data. They are especially concerned about the way sensitive data – like location, activity, children's and health data – is collected, used and sold. And they overwhelmingly want more privacy progress from both policymakers and the companies that provide technologies or control data.

Protecting privacy, and enabling trusted technology is not just integral to our daily lives, it is also essential for fostering solutions to broader societal challenges. When our technologies are broadly trusted and inclusive, they can be more broadly adopted and harnessed to help the administration:

- Tackle our climate challenges
- Bend the healthcare cost curve
- Make farmers more productive
- Ensure our economy is more prosperous
- And create a digital world that is more equitable and inclusive

Trustworthy technologies can't solve all of our challenges, but neither can we solve all of our challenges without harnessing the innovative emerging technologies that can help us tackle some of our biggest issues in novel new ways. We need smart policies for enabling adoption of trusted technologies, and trusted technologies to enable the adoption of smarter policy solutions for a range of societal challenges. Policymakers can start by protecting consumers' privacy and ensuring that the benefits of technology are broadly available for all Americans. These are key to fostering the trust necessary for achieving these goals in more inclusive ways.

NEED TO FOCUS ON PARTICULARLY SENSITIVE DATA AND VULNERABLE POPULATIONS.

Privacy concerns have always been important, but advances in technology in recent years and the way that people use technology in more and more parts of their lives has raised the stakes. Smartphones are increasingly becoming the primary interface to the digital realm with nearly 60 percent of internet traffic now coming from smartphones. We now spend more time using mobile technologies than a desktop. With this transformation, smartphones have become an essential tool for living in today's world.

But as we use our digital devices for more and more purposes, we are creating and storing more and more data. So much so that by the end of 2022, we collectively created and consumed 94 zettabytes of data. Because we are using our smartphones in new and innovative ways throughout our lives, an increasing amount of that data is personal in nature including sensitive information such as bank account information, personal health records, and children's school records.

Given the types of sensitive information people use with their devices, respondents throughout our surveys have indicated they were more concerned about protecting personal data on a smartphone than on a laptop computer. Whether it was banking transactions, health data, information about their children, or photos, about 8 out of 10 respondents want technology companies to do more to keep that information protected.
And virtually no one wants these companies to do less. These numbers were consistent across age, race, and income demographics.

This is why it is more important than ever to comprehensively protect consumer data privacy – especially the most sensitive data we use on our mobile devices.

TARGETING THE MOST VULNERABLE

Unfortunately, as is often the case, our most vulnerable populations bear the brunt of risky or exploitative data practices. Among the many dimensions of digital inequality is the unequal distribution of user privacy protection. For example:

- **Privacy protections are important for low-income Americans.** Low-income Americans are more concerned than their wealthier counterparts about losing control over how their information is collected or used. One study by the Data & Society Research Institute found that 60% of those in the lowest-income households say the loss or theft of financial information is something they are "very concerned" about, while just 38% of those in the highest-earning households say the same. At the same time, identity theft poses a much heavier burden for people living on the margins, one comprehensive survey found.

- **Privacy protections are important for people of color.** The cybersecurity firm Malwarebytes found Black people, Indigenous people, and People of Color (BIPOC) are more likely to have their identities stolen than White people: 21 percent compared to 15 percent. They found among those who are victims of cyber crimes, BIPOC people are the least likely to avoid any financial impact due to cybercrime: 47 percent compared to 59 percent of all respondents.

- **Privacy protections are important for seniors.** Seniors are another group who stand to benefit from new technologies, but as Pew Research reports, while 96% of those ages 18 to 29 own a smartphone only 61% of those 65 and older do, a 35 percentage point difference. Why the gap? AARP research found 34 percent of people age 50 and older cite privacy concerns as a top barrier to adopting new technology with more than 8 in 10 (83 percent) indicating they are not confident that what they do online remains private. Our own Trusted Future survey found that virtually no one (2-3%) over the age of 55 felt confident in their ability to protect their own data. This lack of trust may be why seniors are often targeted by increasingly sophisticated online schemes aimed at stealing personal information or financial information through deceptive and socially engineered communications like phishing, or its text message counterpart called smishing.

- **Privacy protections are important for women.** Women's privacy issues are also critical, and have become more more pronounced following the decision in the Supreme Court ruling in Dobbs v. Jackson Women's Health Organization, which overturned Roe v. Wade. As Senator Ron Wyden describes the new problem, "Your geolocation data, apps for contraception, web searches, phone records—all of it is open season for generating data to weaponize the personal information of women across the country." Our own Trusted Future Survey found that 82% are concerned about their private data being sold without their consent or shared with others without their permission. In fact, 59% want the messages between them and their doctors to be protected with strong encryption that ensures that no one but the author and the intended recipients is able to read the message.

- **Privacy protections are important for LGBTQ Americans.** For many LGBTQ Americans, privacy is crucial and strong encryption is a critical part of that equation. As LGBT Technology Partnership's Carlos Gutierrez has observed, "A privacy data breach that exposes someone's sexual orientation can have far-reaching effects, including the loss of employment, loss of familial relationships and friendships and even the potential for physical harm or death."

- **Privacy protections are important for everyone.** Privacy protections aren't just critical for vulnerable and marginalized communities, they are important for every American. Our own Trusted Future survey found that 62% of Americans are very concerned about protecting their privacy from unscrupulous actors. Only 16% of Americans feel firmly in control of their data.

RESPONSE TO QUESTION 2: "ARE THERE SPECIFIC EXAMPLES OF HOW COMMERCIAL DATA COLLECTION AND PROCESSING PRACTICES MAY NEGATIVELY AFFECT UNDERSERVED OR MARGINALIZED COMMUNITIES MORE FREQUENTLY OR MORE SEVERELY THAN OTHER POPULATIONS?"

In its request for comment, NTIA has asked the important question about examples of how commercial data collection may negatively affect underserved or marginalized communities compared to other populations.

As smartphones have become a primary digital onramp for vulnerable populations, and they have become the technological tool that often contains the most sensitive personal data, they have become the primary front line tool for protecting privacy and security. Thus efforts to address privacy and equity must address the needs for robust security and privacy on mobile devices in order to protect every user.

Today, some smartphone apps can undermine people's privacy by tracking them across apps, and across town revealing potentially intimate secrets. In 2018, The New York Times conducted an experiment highlighting just how invasive data tracking can be. In the expose, titled Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret, The Times gained access to commercially available data, and using basic data analysis techniques was able to track individuals during some extremely personal activities. Just some of the examples from this single data set include:

- One path that tracks someone from a home outside Newark to a nearby Planned Parenthood, remaining there for more than an hour.
- Another represents a person who travels with the mayor of New York during the day and returns to Long Island at night.
- A teacher is tracked going to school, going to a weight watchers meeting, and to a dermatologist – all without her knowledge.
- Even the former President's location was tracked during the 2017 inauguration based on the pings of the people who were surrounding him.

As one U.S. Senator described the challenge: "Location information can reveal some of the most intimate details of a person's life — whether you've visited a psychiatrist, whether you went to an A.A. meeting, who you might date."

While some companies have put in place efforts to try and protect user privacy, others have gone to great lengths to try and exploit sensitive smartphone data. For example in 2015, Uber went to great lengths in an attempt to get around key privacy protections built into Apple's App Store. According to New York Times reporting and a book by the same author detailing it, Uber knew that accessing cameras, messages, contacts and GPS even after the Uber app was closed was exactly the kind of consequential privacy violation that could get it kicked out of Apple's app store, in fact, a previous Uber app update was rejected by Apple over fundamental privacy violations.

However, rather than fixing the privacy problems, the company developed a complicated scheme to hide its privacy-violating code deep within the app and then make it undetectable to Apple engineers. To hide it, they created a digital fence around Apple's headquarters in Cupertino called a geofence. Inside the fence, the privacy violations did not occur. But outside the geofence, the code allowed Uber to continue to collect the data and violate privacy rules. Apple engineers eventually uncovered the scheme and determined that Uber was violating App Store rules and was also purposefully trying to evade compliance. Only after the two CEOs met and Apple threatened to pull Uber's app from its store Kalanick decided to fix the problems. Previously they had used this kind of data to track and post about its user's one night stands.

While the commercial sale of personal data, and efforts to exploit privacy are too commonplace and affect nearly every community, they are often more acute and exploitative for vulnerable and underserved communities. In fact, some of the most harmful examples of privacy violations target such communities.

Some examples where personal data was exploited from potentially vulnerable populations:

- **Exploitation of personal data of LGBTQ+ community members:** The dating app Grindr that serves the LGTBQ+ community provides a powerful example of the ways in which personal data can be collected and sold beyond the expectations of its users. Last year, The Wall Street Journal reported that the precise movements of millions of Grindr users were collected from a digital advertising network and made available for sale. The data didn't contain specific personal information such as names or phone numbers, however by analyzing patterns of the location data, in some cases it was possible to determine people's identities based on their workplaces, home addresses, and habits and routines. It was even possible to determine romantic encounters between specific users based on their device's proximity to one another. While Grindr does not sell ads in countries where there are laws against homosexuality, such data could be – and has been – used for blackmail against those who are not living openly. A famous example occurred in 2021 when a Catholic publication called The Pillar said it obtained commercially available data that allowed it to track Grindr usage by individuals, leading to a senior official of the U.S. Conference of Catholic Bishops to resigning after he was approached and identified as a user of the app.

  In a study conducted last year by Lawfare titled "Creating a Framework for Supply Chain Trust in Hardware and Software," they looked at how the app's data was handled after collection and found that Grindr was communicating with fifty-three different unique domains and thirty-six different advertising companies, with eleven parties receiving the user's exact GPS location, four parties receiving the user's IP and/or MAC address, and seven parties receiving "personal information about the end user, such as age or gender."

- **Harvesting of personal information collected by a Muslim prayer app that was sold to U.S. military and defense contractors.** In 2020, Vice's Motherboard reported that the U.S. military and defense contractors were buying the granular movement data of people around the world, often from innocuous-seeming apps. The most popular app connected to this effort was a Muslim prayer and Quran app that reminds users when to pray, what direction Mecca is in relation to the user's current location, where to find local halal food, and aids in fasting during the holy month of Ramadan. It had been downloaded over 98 million times by the time the reporting came out. A Muslim dating app that had been downloaded 100,000 times at the time of the public revelation of the program was also part of the effort, as were other apps. According to the Motherboard reporting, U.S. Special Operations Command (USSOCOM), a branch of the military tasked with counterterrorism, counterinsurgency, and special reconnaissance, bought access to the data to assist on overseas special forces operations.

In each of these privacy examples involving Uber, Grindr and the Muslim prayer app – **the use of an advertising ID is at the heart of efforts to track activity and connect data.** These advertising IDs – a unique number used to identify a specific phone – are at the heart of mobile data tracking, and the multi-billion dollar data broker industry built around it to track a device, combine disparate data about the devices and its users to create detailed profiles. The third party data brokers use the unique advertising ID to combine it with other information about you – like location data, age, income, marital status, and proclivities – to create a substantially more detailed profile about you that they can then resell for marketing purposes. When combined with other data, a device's advertising ID data can reveal some of the most intimate details of a person's life. These trackers have become commonplace, and can be found in two-thirds of the most popular apps used by children, in popular dating apps, prayer apps, and period tracking apps.

Many smartphone users have recently been given the power to "ask Apps not to Track" as a way of disabling the use of these advertising IDs – which has proven to be highly popular as measured by its high adoption rates. In the wake of the Supreme Court's Dobbs decision, the U.S.Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued guidance to help women protect their privacy by limiting the collection of location data, and for taking steps to prevent the advertising ID from tracking user activity.
Nonetheless, some app developers have tried to get around these app store based advertising ID restrictions by combining a number of other pieces of data from a smartphone – beyond the basic data needed to provide a specific service – to create an alternative unique digital fingerprint that can be used to identify a specific user and its device. Others have supported efforts to get around app store restrictions that limit digital fingerprinting and require apps to display the "ask App not to Track" prompt by requiring smartphone makers to allow app sideloading – effectively creating a back door way around smartphone privacy restrictions. Without a comprehensive, effective,and enforceable national privacy framework in place first, any steps to undermine existing digital fingerprinting prevention review mechanisms or that give bad actors a backdoor way around privacy restrictions that prevent exploitation of advertising IDs could impede efforts to protect privacy – especially for the specific vulnerable populations that have already seen their privacy exploited through widespread collection of the advertising IDs.

Such examples of personal data being commercially exploited are concerning privacy violations on their own. However, the broader implications they have on limiting trust in technologies for these underserved, disadvantaged, and marginalized populations could have even deeper long term impacts. If vulnerable communities cannot trust that data collected about them through the use of common apps will not be exploited, then they are less likely to adopt the new technologies that might be beneficial and could improve their lives and thus risk being left further behind.

RESPONSE TO QUESTION 4: "HOW DO EXISTING LAWS AND REGULATIONS ADDRESS THE PRIVACY HARMS EXPERIENCED BY UNDERSERVED OR MARGINALIZED GROUPS? HOW SHOULD SUCH LAWS AND REGULATIONS ADDRESS THESE HARMS?"

NTIA's request for comment asks specifically about existing laws and regulations to address harms toward underserved communities. There are several key steps the administration can take to elevate its privacy policy process, and improve outcomes for underserved and marginalized groups using its existing authorities.

- **First, the Administration should take a whole of government approach to improving privacy progress for all – including underserved and marginalized groups.**

  The administration can and should create a new interagency commercial data privacy working group/council to elevate its focus on these issues, coordinate progress more effectively across agencies, better align policy approaches to ensure other priorities don't marginalize efforts to improve consumer data privacy for critical groups, to enable stronger collaboration and sharing of cross agency expertise, and to more effectively support congressional efforts in advancing a comprehensive federal privacy framework.

  Not only can such an effort elevate privacy priorities, but it can also help ensure that the administration's privacy efforts are more closely aligned with its cybersecurity approach, its encryption policy, to boost competition, and improve equity, diversity and inclusion. It can also help the agencies consider privacy impact around new emerging technologies, and proactively think through potential efforts as technology is more broadly employed through efforts and segments that a broader range of agencies are focused on – in for example banking, transportation, agriculture, energy, communications, housing, and building.

  Such an effort can also help boost international privacy coordination where, for example, European Union efforts to promote digital markets, unless properly informed and tempered, could end up weakening private and secure encrypted communications impacting the privacy and security of marginalized American users too. Elevating the administration's approach to improving consumer privacy can have generative impacts too – whereby one good administration action (elevating the issue throughout the administration) becomes a powerful tool for generating other good policy outcomes.

- **Second, the Administration should elevate its privacy enforcement efforts.**

  There are key steps the Administration has already taken, that can be built upon, to help drive more expansive privacy protections for vulnerable populations. For example, after the Supreme Court's decision in Dobbs v. Jackson Women's Health Organization, which overturned Roe v. Wade, the White House took key steps to elevate action and better protect people's privacy when using a mobile device. The White House Fact sheet accompanying the order indicates: "The President has asked the Chair of the Federal Trade Commission to consider taking steps to protect consumers' privacy when seeking information about and provision of reproductive health care services." Following this order, the Federal Trade Commission (FTC) took the important step of suing a data broker that tracks locations of 125M phones per month (which included the use of advertising IDs) which can be used to track the movements of people visiting abortion clinics, domestic abuse shelters, places of worship, and other sensitive places. Using the regulatory tools of the FTC to curb privacy violations is an example of ways that the executive branch can help address such harms absent legislation from Congress.

Similarly, in 2021 the FTC took action to ban the stalkerware app SpyFone and its CEO Scott Zuckerman from the surveillance business over allegations that the app company was secretly harvesting and sharing data on people's physical movements, phone use, and online activities. In this case, the app at issue was not approved by official app stores but instead had to be downloaded from a third-party website and sideloaded onto mobile devices that allowed sideloading. Once downloaded, the app then "surveilled physical movements, phone use, online activity through a hidden hack that exposed device owners to stalkers, abusers, hackers, and other threats," according the FTC. The FTC found "The company's apps sold real-time access to their secret surveillance, allowing stalkers and domestic abusers to stealthily track the potential targets of their violence." They found "SpyFone's lack of basic security also exposed device owners to hackers, identity thieves, and other cyber threats."

Policymakers can build on this effort by encouraging developers to be fully transparent about their privacy practices in the information they submit for purposes of consumer privacy labels, and encourage app store providers to further improve upon their app store review processes to root out these kinds of nefarious apps and app features. In its complaint against SpyFone, the FTC specifically noted how consumers were tricked into disabling certain mobile device security features in order to download the nefarious app from outside of official app stores (aka sideloading).

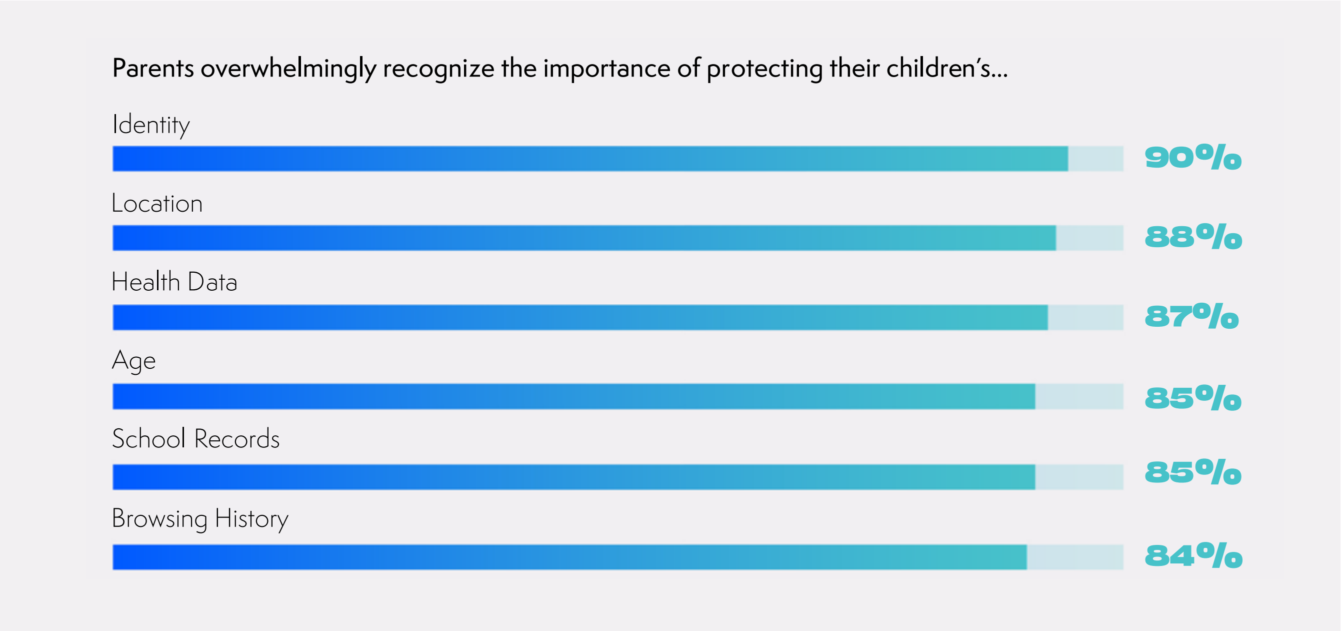
To further protect consumers, the FTC can take further action against these and other bad actors who attempt to exploit the consumer privacy of vulnerable populations. The FTC and the Commerce Department can also improve consumer awareness of these potentially harmful sideloaded apps by further evangelizing among vulnerable populations the FTC's tips: "How To Protect Your Privacy on Apps" which provide consumers with helpful tools and steps to better protect their privacy.

- **Third, the Administration has within reach other regulatory proceedings that can improve privacy for vulnerable populations.**

Protect student data privacy: To better protect children's privacy, the Federal Communications Commission is currently considering an important proposal to allow federal E-Rate funding to be used to improve school cybersecurity in order to better protect student and staff data. A spate of recent attacks has disrupted education, and jeopardized the privacy of students and staff.

It also comes at a time when an international investigation that found educational tools used by students during the pandemic shared their information with advertisers and data brokers at a "dizzying scale." According to The Washington Post, "Researchers found the tools sent info to nearly 200 ad-tech companies, but few programs disclosed to parents how companies would use it. Some apps hinted at monitoring in technical terms in their privacy policies [while] others made no mention at all." The "study identified code in the app that would have allowed it to extract a unique identifier from the student's phone, known as an advertising ID, that marketers often use to track people across different apps and devices and to build a profile on what products they might want to buy," according to The Post.

These are critical issues. Our own Trusted Future survey found that 85% of parents think it's important to keep their children's school records safe and 90% want their identities secured. They overwhelmingly want the devices their children use to meet robust cybersecurity standards and they support efforts to limit cyber threats like malware and ransomware.


Parents overwhelmingly recognize the importance of protecting their children's...

To better protect student data privacy and security, as the President's primary voice on telecommunication policy matters, we would encourage NTIA to file comments with the FCC in support of improving student security and privacy through the federal E-Rate program.

Improve Mobile Provider user data privacy. As for mobile service providers, the Federal Communications Commission can also look more closely at service provider's handling of sensitive customer data, especially location data, data retention, and revisit rules that previously protected people's internet browsing records held by their internet service providers.

As the FCC Chair has said, "Our mobile phones know a lot about us. That means carriers know who we are, who we call, and where we are at any given moment. This information and geolocation data is really sensitive. It's a record of where we've been and who we are. That's why the FCC is taking steps to ensure this data is protected." The FCC Chair has also asked its Enforcement Bureau to launch a new investigation into mobile carriers' compliance with FCC
rules that require carriers to fully disclose to consumers how they are using and sharing geolocation data.

These steps can be supported, and can enable further privacy progress. Our own Trusted Future survey finds that consumers are more likely to trust their connected technologies when companies are prevented from collecting and selling sensitive location and other sensitive information without their explicit consent (59% support).

RESPONSE TO QUESTION 6 "What other actions could be taken in response to the problems outlined in this Request for Comment?"

- **First, the U.S. needs a comprehensive federal privacy framework that protects all Americans, and the Administration can help catalyze action.**

  Today far too many Americans lack baseline protections for their sensitive personal information. Consumers, patients, children, and innovators all deserve more certainty and a comprehensive national framework to guide how data is minimized, collected, protected, accessed, transferred and governed. We support efforts to help make privacy a basic digital right. And while some states have stepped forward on privacy, we agree with NTIA Administrator Alan Davidson that your privacy rights shouldn't change when you cross state lines.

  We also agree with the President when he says, *"we need serious federal protections for Americans' privacy. That means clear limits on how companies can collect, use and share highly personal data—your internet history, your personal communications, your location, and your health, genetic and biometric data."*

  Our own Trusted Future survey confirms consumers want comprehensive privacy protections written into law (46%). To make progress, the number one thing that the Administration can do is build on last year's congressional efforts towards comprehensive privacy legislation. Bipartisan, bicameral congressional leaders built upon a growing consensus that we need to better protect consumer privacy by minimizing data collection, increasing transparency and user control of data, addressing digital tracking concerns, and moving towards a world where data protection is built-in to our technologies by design.

  When Trusted Future asked consumers what technology policy issues they wanted Washington to prioritize, a significant majority (63%) said Congress should prioritize legislation that will provide users with additional privacy protections, whether it specifically be children's privacy (37%) or a broader national privacy framework (26%).

  In terms of the kinds of privacy protections consumers would like to see, our surveys have shown that a strong majority of Americans:

  - Want data minimization, limiting data collection beyond what is needed for the app to function.
    - » **59%** want companies to be prevented from collecting and selling sensitive location and other sensitive information without your explicit consent.
    - » **71%** support requiring companies to only collect the minimum amount of data necessary to deliver their services.
  - Want privacy labels for products
    - » **45%** want easy to use privacy labels that help them understand what data is being collected and shared by the apps they use.
  - Seek specific protections for kids, including:
    - » **75%** support the ability to delete data collected about children,
    - » **73%** want to extend the same rules governing children's privacy to teenagers
  - Recognize the importance of encryption, on the device, in communication, and in the cloud.
    - » **59%** want the messages between you and your doctors to be protected with strong encryption

that ensures that no one but you and your intended recipients are able to read your messages.

  - **52%** want the personal health data you have stored to be backed up in an encrypted way ('lock box') where only you have the key to unlock it.
  - They also want policymakers to reject efforts that have the effect of weakening strong encryption, and encourage the efforts of companies to protect their customers by deploying strong encryption **(52%).**

- **Second, absent legislative action, the Administration should work to accelerate private sector privacy progress.**

Even in the absence of comprehensive legislative action, there are concrete steps companies can take today to boost consumer privacy protections – and the Administration can help use its bully pulpit, its expertise and convening power to help accelerate more private sector progress. Trusted Future's survey shows that 7 out of 10 consumers want companies to do even more than they already do to protect privacy. They want companies to minimize data collection, use strong encryption, build comprehensive privacy protections into devices, apps, and services, and not collect or sell location and other sensitive information without their consent. In many cases, private sector action can happen faster than the legislative or regulatory process itself.

The Administration should encourage competition between companies based on the level of privacy and security they provide, continuing to transform trusted technology into a competitive advantage in the marketplace.

- For example, McKinsey's Why Digital Trust Truly Matters, found that companies that lead in building digital trust can increase annual growth by 10 percent or more. It shows how companies that build digital trust can have a competitive advantage in the marketplace.
- Similarly, the KPMG 2022 'Cyber Trust Insights' report found that 1/3 of organizations in a survey already recognize that increasing consumer trust through steps like better privacy can improve profitability. They found that companies can help foster trust by focusing on improving cybersecurity, privacy and reliability; by ensuring inclusive ethical and responsible use; by driving accountability; and providing oversight on its trustworthiness efforts.
- PwC found boosting trust in technology can help give companies a competitive advantage, and McKinsey similarly found those companies that are leaders in building digital trust can increase annual growth by 10 percent or more.

But surveys also show too many companies have not yet established a digital trust framework nor have they designated a Chief Trust Officer. For example:

- ISACA's State of Digital Trust, found that 51% say having a Digital Trust Framework is very or extremely important, but 24% do not have a senior staff role dedicated to digital trust.
- A Deloitte study on trust and ethics in technology reveals that while business leaders are aggressively moving forward on implementing and using emerging technologies, nearly 90% of those surveyed lack a framework to support the implementation of ethical principles to guide its development and use. (Full report here)

These surveys show that improving privacy, security, trust and inclusion can boost a company's bottom line, and help to create a competitive advantage in the marketplace. But they also show consumers want companies to do more, and too few companies have taken key baseline steps to help foster trust – steps like minimizing data collection, building technologies that are secure by design, adopting NIST risk-management frameworks, prioritizing privacy across the organization, developing a company-wide digital trust framework, and appointing senior staff roles in charge of trust. The Administration can take immediate steps, even in the absence of a new legislative framework, to convene and encourage greater private sector action. Because when companies compete on trust, consumers and businesses can both win.

CONCLUSION:

The administration has within its reach an opportunity to make major progres to improve the lives of millions of Americans by focusing on advancing privacy progress. We look forward to working with the NTIA and the Administration on ways to improve trust in technology in order to ensure that all Americans – regardless of income, geography, or circumstance – are able to protect the privacy of their data, and able to benefit from the opportunities that trusted technologies can enable.