Before the
National Telecommunications and Information Administration
U.S. Department of Commerce
Washington, D.C.

In the Matter of	
Request for Comments on Developing the Administration's Approach to Consumer Privacy	Docket No. 180821780-8780-01

COMMENTS OF THE
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

John A. Howes, Jr.
Jacqueline Yin
Computer & Communications
Industry Association (CCIA)
655 15th Street, N.W., Suite 410
Washington, D.C. 20005
(202) 783-0070
jhowes@ccianet.org

November 7, 2018

Before the
National Telecommunications and Information Administration
U.S. Department of Commerce
Washington, D.C.

In the Matter of	
Request for Comments on Developing the Administration's Approach to Consumer Privacy	Docket No. 180821780-8780-01

COMMENTS OF THE
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)[1]

Pursuant to the request for comments (RFC) issued by the National Telecommunications and Information Administration (NTIA),[2] the Computer & Communications Industry Association (CCIA) submits the following Comments. The RFC offers an in-depth look at consumer privacy expectations, suggesting certain outcomes and setting high-level goals that describe the outlines of an ecosystem that should be created to provide those protections. In these Comments, CCIA addresses how these privacy outcomes and goals can be achieved. Furthermore, CCIA seeks to inform the Administration on future policy, actions, and engagement on consumer privacy. Any outcomes or goals developed by NTIA, the Administration, or Congress as a result of this RFC should (1) aim to protect data through a robust, technology-neutral framework for assessing and managing privacy risks to individuals and organizations; and (2) seek to promote innovation in both digital services and privacy

[1] CCIA represents large, medium, and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications, and Internet products and services. Our members employ more than 750,000 workers and generate annual revenues in excess of $540 billion.

[2] Notice, *Request for Comment on Developing the Administration's Approach to Consumer Privacy*, 83 Fed. Reg. 48600 (Sept. 26, 2018).

protection. Included as an addendum to these Comments, CCIA provides its "Privacy Principles" to help guide the development of a national policy on consumer privacy.

As the world becomes increasingly data-focused, attention has inevitably shifted to the impact of data on consumers and whether and how improvements should be made. Recent controversies have shifted how companies and consumers think about how data is collected and used online, generating some positive responses in terms of practice and transparency. It is important for the U.S. to have a healthy data ecosystem with transparency and accountability, which will help drive innovation and U.S. competitiveness.

CCIA supports the development of baseline, Federal privacy legislation that would ensure that data is handled responsibly and with transparency while also ensuring that consumers can benefit from innovation and new technologies. Such a framework should be technology-neutral, meaning it should not provide specific technology mandates; sector-neutral, meaning it should apply to online and offline companies; and it should provide for safe harbors and flexibility for companies to make adjustments according to the needs of consumers.

Given the complexity and sensitivity of issues related to consumer data privacy, any Federal policy will require sufficient input from all stakeholders and clear definitions to ensure careful implementation. Therefore, CCIA applauds NTIA and the Commerce Department for conducting this Comment process and for seeking broad engagement and input from stakeholders and the public on ways to advance consumer privacy while protecting prosperity and innovation. NTIA has a unique ability to address this issue due to its position within the Executive Branch as the President's principal advisor on telecommunications and information policy issues, its extensive experience with these issues due to its international engagement, and its ability to engage with outside groups. Although sudden action by the U.S. government could adversely impact innovation for online services and privacy controls, leading to stark choices by

small and new firms, CCIA encourages NTIA and the Commerce Department to continue pursuing a constructive dialogue from a wide variety stakeholders and the public.

I. Introduction.

The Internet is a revolutionary engine of economic growth – a unparalleled catalyst for innovation, providing entrepreneurs with access to markets that were previously unreachable. A major factor of this economic development and growth has been the free flow of data and information. Indeed, by one measure, fifteen to twenty percent of GDP growth in many countries, including developing countries, can be attributed to the Internet and associated data flows.[3] However, this growth can only occur and can only continue if consumers and businesses trust that the personal data they provide to other businesses will be safeguarded. User trust is essential.

Organizations across the digital ecosystem use personal data to provide innovative services. Responsible data use can be beneficial for people, businesses, and society. Analysis of consumer data allows companies to better understand what products customers like, which helps companies improve their products and services, provide recommendations for others that consumers may also like, and create new products and services. When evaluating the reasonability of an organization's data protection practices, it is important to understand the context in which an organization collects, processes, and uses personal information. This context can include the nature of the relationship between an individual and the organization, the potential benefits an individual, organization, and society might receive from particular uses of information, and individuals' expectations regarding data protection.

[3] *See* Andrew McAfee & Erik Brynjolfsson, *Big Data: The Management Revolution,* HARV. BUS. REV. (Oct. 2012).

Consumers also depend on organizations to use their data responsibly and be transparent about what they are collecting and how they are collecting and using it. Therefore, organizations must respect individuals' interests when they process personal information. Organizations should make reasonable best efforts to account for and mitigate potential harms to individuals, communities, and society. Reasonable data protection measures that align with individuals' expectations can protect people and communities from harms that result from misuse of data and help maintain the trust between consumers and organizations.

II. Privacy Outcomes.

The RFC presents seven policy outcomes for organizations that handle consumer data as the Administration attempts to "refocus on the outcomes of organizational practices, rather than on dictating what those practices should be."[4] In this response, CCIA attempts to address the proposed outcomes in the order they were presented but also adds data portability as another outcome that is important for this discussion.

A. Transparency.

CCIA appreciates that NTIA seeks to promote flexibility in its approach to transparency. Organizations must be transparent about what personal information they are collecting, why they are collecting it, and how they are using it. However, as NTIA notes, lengthy notices describing privacy policies frequently do not lead to adequate understanding for consumers. Organizations should make privacy policies clear, concise, and easy to understand. Furthermore, they should make reasonable efforts to actively inform individuals, making the information relevant and actionable, about data use in the context of the relevant services. Examples of ways to promote transparency include updating privacy policies with informational videos and allowing for privacy controls to be easy to find and immediately accessible through an organization's privacy

[4] RFC at 48601.

policy. In addition, organizations should be clear about whether personal information may be transferred to third parties, how long that information may be retained, and what choices and controls individuals have with respect to their personal information.

B. Control.

CCIA agrees that "[u]sers should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide to organizations."[5] Organizations must provide appropriate mechanisms for individual control, considering the service, and CCIA agrees that controls "should be developed with intuitiveness of use, affordability, and accessibility in mind, and should be made available in ways that allow users to exercise informed decision-making."[6] Individuals should be able to object to data processing where it is feasible, but policymakers should be wary of requiring individuals to control every aspect of data processing. Policymakers should avoid requiring specific consent for every use of data, which could create an overly complex and confusing experience for the individual and divert from the overall goals that the policy seeks to achieve. Policymakers should also keep in mind that the responsible processing of personal information is necessary to simply operate some services.

C. Security and Risk Management.

Users should expect that organizations handling their data will do so carefully and responsibly with reasonable measures to protect personal information from unauthorized access, misuse, modification, disclosure, loss, and destruction. CCIA agrees that risk management is essential and appreciates NTIA's attempt at enabling "flexibility to encourage innovation in business models and privacy tools, while focusing on potential consumer harm and maximizing

[5] *Id.*
[6] *Id.*

privacy outcomes."[7] Policy should account for and be proportionate to the risk of harm. Organizations should follow consensus best practices, and if a security breach occurs, organizations should notify individuals expeditiously when there is a significant risk of harm.

D. Access and Correction.

Individuals must be able to access the personal information that they have provided to an organization, and it should be made available for export in a machine-readable format. Organizations should afford users with the ability to correct and/or delete the data that they provide to that organization when it would be practical and provided that deletion would not implicate the personal information of others. Data access and correction tools, where appropriate given the nature of the service, can help organizations meet this obligation. Personal information should be accurate, current, and complete to the extent possible for the purpose for which the organization maintains the data. There should also be appropriate limits for legitimate need or to meet legal obligations.

E. Accountability.

CCIA agrees that "external accountability should be structured to incentivize risk and outcome-based approaches within organizations that enable flexibility, encourage privacy-by-design, and focus on privacy outcomes."[8] Organizations should regularly assess the privacy risks associated with their collection, processing, and use of personal information; develop systems to mitigate risks in a reasonable and proportionate manner; and monitor services for bias and disparate impacts. Indeed, organizations should practice privacy by design, building products and services that prioritize privacy, security, reliability, and reduce the likelihood of vulnerabilities, which will help earn user trust. Lawmakers and regulators should set baseline

[7] *Id*. at 48602.
[8] *Id*.

requirements, but they should also enable flexibility to meet those requirements and promote industry accountability programs and safe harbors.

F. Data Portability.

Data portability is the capability to migrate personal data that a user has shared with one organization to another. Data portability facilitates competition and innovation by making it easier for consumers to try new products and services without being locked into using an existing service. Interoperability is also an important means of enhancing user choice and control. Consumers may want to ensure that their information is protected and secure and that that information has the ability to go with them should they choose a new or competing service.

Any conversation on data portability, interoperability, privacy, and security involves complicated technical and competitive factors. Chief among those factors is determining the appropriate scope of data to be made portable and the extent of interoperability for particular services. Organizations should make reasonable efforts to enable authenticated users to obtain data they provide to that organization for their own purposes or for use with a different organization or service, provided that these data portability tools do not implicate the personal information of others. Data transfers between covered organizations should be private, secure, and balanced. Data portability tools should: (1) allow users to download and move data they have provided to the service, but not data that may relate to other users; (2) afford users control over how and when the tools are used; and (3) be tailored to the privacy and security expectations of specific products and services. Further, data portability tools should enable machine-to-machine transfers where technically feasible.

III. High Level Goals for Federal Action.

With those outcomes in mind, currently, there is a desire to bring the power of the government to bear on consumer privacy. Nevertheless, privacy regulation must be balanced against the need to encourage innovation and the societal impact of big data. Restricting companies' use and collection of data may unintentionally impair commerce in the digital economy, and by implication, reduce investment. This especially affects firms that rely on the collection, analysis, or storage of large amounts of user data, such as companies in the cloud computing, online news, and online advertising sectors. These sectors are highly relevant to the online consumer experience as they encompass many of a user's typical online interactions. However, it is not just large companies that process and use personal data – charities, nonprofits, and community organizations would also be impacted depending on how government regulation of consumer data is defined and applied. Indeed, over-regulation or enhanced restrictions on data collection and usage could hinder the development of research and science that can benefit society.[9]

As with innovation, there are parallel risks to competition if privacy laws and regulations are not appropriately designed. Due to economies of scale, larger companies can better bear the costs of complying with the same regulations as smaller companies and new market entrants – before even mentioning nonprofits – especially in the privacy context.[10] It is also important to consider that, insofar as privacy regulations function to inhibit voluntary portability of users' data from one service to another, these regulations may cut against open, horizontal business

[9] *See* Ford, B., et al., *Status update: is smoke on your mind? Using social media to assess smoke exposure*, 17 Atmos. Chem. Phys. 7541-7554 (2017), https://doi.org/10.5194/acp-17-7541-2017 (using social media post to improve traditional methods of assessing population-level exposure to fires in the Western U.S. during the summer of 2015).

[10] *See* James Campbell, Avi Goldfarb, & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRATEGY 47 (2015).

models and indirectly favor closed, vertical models. Therefore, regulations should be proportionate to the risk of harm and permit flexibility in compliance.

Over-regulation risks the possibility of creating too many high barriers to entry for new services and may even prohibit the creation of services that users might desire and that use personal data respectfully. Indeed, studies have shown that while privacy regulations impose costs on all covered organizations, small and new firms suffer the most, especially in ad-supported industries.[11] Professor Anja Lambrecht of the London Business School found that earlier privacy laws in the EU depressed relative venture capital investment, compared to the U.S., by fifty-eight to seventy-five percent annually in the years after the 2002 e-Privacy Directive.[12] Indeed, there are indications that investment has sharply declined in Europe as a result of the EU's General Data Protection Regulation (GDPR).[13] This trade-off between regulation and growth and investment may be acceptable in some countries but not in others.

However, action by the U.S. government on consumer privacy will not automatically suppress innovation or economic activity. Ensuring privacy rules are designed thoughtfully, so that requirements are scalable and context-dependent, can help promote competition and data protection goals. As U.S. policymakers consider whether and how privacy and data security should be addressed at the federal level, any action should: (1) aim to protect data through a robust, technology-neutral framework for assessing and managing privacy risks to individuals and organizations; and (2) seek to promote innovation in both digital services and privacy protection.

---

[11] *See, e.g.*, James David Campbell, Avi Goldfarb, Catherine E. Tucker, *Privacy Regulation and Market Structure* (Dec. 22, 2010; last revised Nov. 8, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1729405.

[12] *See* Anja Lambrecht, *E-Privacy Regulations and Venture Capital Investments in the EU*, DISRUPTIVE COMPETITION PROJECT (Jan. 15, 2018), https://www.project-disco.org/privacy/011518e-privacy-regulations-venture-capital-investments-eu/.

[13] Jian Jia & Liad Wagman, *Data as a Driver of Economic Efficiency*, DATA CATALYST (Nov. 2018), https://datacatalyst.org/reports/data-as-a-driver-of-economic-efficiency/.

A. Harmonize the Regulatory Landscape: Comprehensive Baseline Privacy Legislation.

Congress should hold hearings and take input from a broad range of stakeholders from industry, civil society, consumers, and academia to develop carefully crafted, comprehensive, baseline privacy legislation that provides clear standards for organizations and ensures that users can expect consistent data protections from organizations that retain their data. Federal legislation should ensure that data is handled responsibly and with transparency while also ensuring that consumers can benefit from innovation and new technologies.

A national, privacy framework should be consistent throughout the United States, so state laws on matters concerning data privacy, security, and breach notifications should be preempted where appropriate. However, it should allow for enforcement by state attorneys general where the FTC has declined to act. Such a framework should be technology-neutral, meaning it should not provide specific technology mandates; sector-neutral, meaning it should apply to online and offline organizations; and it should provide for safe harbors and flexibility for organizations to adjust according to the needs of individuals and evolving technologies.

1. FTC as the Primary Privacy Enforcement Agency.

Comprehensive baseline privacy legislation should be enforced primarily by the Federal Trade Commission (FTC) at the Federal level because the FTC is the Federal agency with the most experience and expertise in the privacy and data security context. The FTC has generally wielded its authority to deter unfair and deceptive acts and practices in a balanced manner that seeks to protect privacy while also promoting innovation. Indeed, the FTC has brought more

than one hundred privacy and data security cases, and it has issued dozens of reports involving privacy and security.[14]

The FTC can use a variety of remedial approaches to protect consumers' privacy and personal information. The FTC's primary authority derives from its ability to protect consumers from "unfair and deceptive acts and practices in commerce" under Section 5 of the Federal Trade Commission Act.[15] The FTC also has authority to enforce a variety of sector-specific laws as part of its privacy and data security or consumer protection toolkit, including the Truth in Lending Act,[16] the CAN-SPAM Act,[17] COPPA,[18] the Equal Credit Opportunity Act,[19] the Fair Credit Reporting Act,[20] the Fair Debt Collection Practices Act,[21] and the Telemarketing and Consumer Fraud and Abuse Prevention Act.[22] Indeed, one of the FTC's principal tools is to bring enforcement actions to stop violations of the law and require companies to take affirmative steps to remediate unlawful behavior. The FTC can also seek civil monetary penalties for violations of an order.[23]

This approach allows it to enable innovative privacy and security practices not previously envisioned. The FTC's long-standing practice of engaging in data-driven analyses is the key to balanced and effective consumer protection, and it will protect against the risk that the FTC

[14] *See* Federal Trade Commission, *Privacy & Data Security Update (2017): An Overview of the Commission's Enforcement, Policy Initiatives, and Consumer Outreach and Business Guidance in the Areas of Privacy and Data Security*, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf.
[15] 15 U.S.C. § 45.
[16] 15 U.S.C. §§ 1601-1667f.
[17] *Controlling the Assault of Non-solicited Pornography and Marketing*, 15 U.S.C. §§ 7701-7713.
[18] *Children's Online Privacy Protection Act of 1998*, 15 U.S.C. §§ 6501-6506.
[19] 15 U.S.C. §§ 1691-1691(f).
[20] 15 U.S.C. §§ 1681-1681(x).
[21] 15 U.S.C. §§ 1692-1692(p).
[22] 15 U.S.C. §§ 6101-6108.
[23] *See* Fed. Trade Comm'n, *Privacy & Data Security Update (2017)*.

might "erroneously condemn" business practices that provide consumers net benefits.[24] Data-driven reasoning is particularly important in the digital privacy and security context because cost-benefit analysis is a key part of determining whether an allegedly unfair business practice has actually led to substantial injury to consumers or yields overall benefits.[25]

The private sector and consumers would benefit from the FTC's continued engagement with its recent hearings and conferences.[26] The FTC should consider hosting recurring workshops, expanding on its annual PrivacyCon, which has been a productive gathering of government, industry, academics, and civil society to discuss trends and research in the fields of privacy and data security.[27] The FTC should also produce a report on data security, update its guidelines on compliance with its children's privacy rules, and provide a clearer set of rules around the privacy requirements facing organizations when interacting with individuals—without resorting to an enforce-first approach that prescriptively mandates specific conduct and technical standards on the digital ecosystem.

2. The FTC Needs More Resources.

Legislation should provide the FTC with additional resources to conduct the necessary empirical studies to quantitatively evaluate the net consumer benefits and harms of particular business practices to ensure that its regulatory approach is grounded in facts. The FTC's budget

[24] Joshua D. Wright, Comm'r, Fed. Trade Comm'n, *The Economics of Digital Consumer Protection: One Commissioner's View*, Remarks at TechFreedom and International Center for Law and Economics, Washington, D.C. at 6 (July 31, 2014), https://www.ftc.gov/system/files/documents/public_statements/573061/010731techfreedom.pdf.

[25] *See* FTC Policy Statement on Unfairness (Dec. 17, 1980) (appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

[26] Press Release, FTC Announces Hearing on Competition and Consumer Protection in the 21st Century (June 20, 2018), https://www.ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st.

[27] Press Release, FTC Announces PrivacyCon2019 and Calls for Presentations (Oct. 24, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/ftc-announces-privacycon-2019-calls-presentations?utm_source=govdelivery.

request decreased from Fiscal Year (FY) 2018 to 2019,[28] and its budget has declined an estimated five percent over the course of this decade.[29] In FY 2018, the FTC requested the same amount of funding but reduced the number full-time equivalent (FTE) employees working on privacy and identity protection from fifty-four in FY 2017 to fifty-two in FY 2018 and FY 2019.[30] The FTC should be given more authority to police consumer privacy, but it cannot achieve this mission without sufficient funding or personnel.

3. Additional Considerations for Legislation.

Legislation should balance a commitment to baseline privacy principles against the implementation of an overly broad and cumbersome regulation. Meeting specific requirements for the handling, retention, and deletion of personal data may force additional overhead costs and administrative demands on organizations, like startups, that may not have the requisite expertise or resources. Overly prescriptive provisions would require smaller organizations to divert significant resources to record-keeping and compliance instead of innovation and developing new features and better services for users.

B. Avoid Interoperability Mandates.

Organizations and individuals benefit from consistent compliance programs based on widely shared principles of data protection. These principles are intended to be interoperable and consistent with existing cross-border data transfer mechanisms, industry standards, and other cross-organization cooperation mechanisms. Thoughtfully designed portability and interoperability can strengthen user choice and control; however, a lack of careful consideration

[28] Fed. Trade Comm'n, Fiscal Year 2019 Congressional Budget Justification (Feb. 12, 2018), https://www.ftc.gov/system/files/documents/reports/fy-2019-congressional-budget-justification/ftc_congressional_budget_justification_fy_2019.pdf.

[29] David McCabe, *Mergers are spiking, but antitrust cop funding isn't*, AXIOS (May 7, 2018), https://www.axios.com/antitrust-doj-ftc-funding-2f69ed8c-b486-4a08-ab57-d3535ae43b52.html.

[30] *Compare supra* note 28, at 41 *with* Fed. Trade Comm'n, Fiscal Year 2018 Congressional Budget Justification (May 22, 2017) at 39, https://www.ftc.gov/system/files/documents/reports/fy-2018-congressional-budget-justification/2018-cbj.pdf.

can result in tension between users' privacy, security, marketplace competition, and portability. Where operators of interoperable systems may be acting in bad faith, sharing of data can pose privacy risks. Furthermore, mandated interoperability or API access might result in unforeseen anticompetitive consequences that could advantage incumbents over smaller competitors,[31] and could allow some companies to free ride on the efforts of others, chilling the incentive to develop innovative services. Finally, rather than promote competition, mandated interoperability could increase the risk of collusion when competitors are required to collaborate and share information.

C. Ensure the Free Flow of Data.

Cross-border data flows are essential to the modern economy. In the U.S., the productivity gains and efficiencies enabled by data flows have boosted the economy by hundreds of billions of dollars.[32] Cross-border data flows allow Internet platforms and providers to connect small and medium-sized U.S. businesses to a global marketplace. Small businesses and craftspeople located across the U.S. can use platforms like eBay and Amazon to sell their goods worldwide without the need for brick-and-mortar presences abroad.[33] An array of online payment processors and emerging digital currencies allow the same small firms to handle transactions globally, and global Internet advertising networks enable them to target potential customers in markets they would not be able to otherwise access. Larger companies can similarly take advantage of cloud platforms and globally distributed computing resources to analyze vast quantities of data and improve provision of remote services to customers worldwide with benefits visible across industries from manufacturing and retail to finance and healthcare.

---

[31] Chris Riley, *Using Interoperability For Horizontal Competition and Data Portability*, MEDIUM (May 24, 2018), https://medium.com/@mchrisriley/using-interoperability-for-horizontal-competition-and-data-portability6706906ce699.

[32] *See* Bijan Madhani, *Digital Issues in NAFTA: Cross-Border Data Flows and Cybersecurity,* DISRUPTIVE COMPETITION PROJECT (June 15, 2017), http://www.project-disco.org/21st-century-trade/061517-digital-issues-in-nafta-cross-border-data-flows-and-cybersecurity/#.W7ei8hNKjVp.

[33] *Id.*

However, CCIA cautions that while it may seem tempting to use data portability and interoperability as a means of ensuring smaller companies and startups can compete with incumbents, that is not a guaranteed result. For example, new or smaller companies might be unable to match the transfer capabilities of incumbents, to the detriment of their ability to deliver their own services. In addition, data portability tools that are under-resourced may expose users to increased security risk. Frequent, automated collaboration could also lead to inadvertent collusion and information sharing between interoperable services. Instead, Federal policy should encourage cross-border data transfer mechanisms, support the development of industry standards, and promote other cross-organization cooperation mechanisms.

D. Promoting Best Practices.

Federal policy should create incentives for organizations to advance privacy protections and find new ways to promote responsible data collection and use. Policymakers should provide flexible approaches to dealing with emerging and evolving technologies; for example, government can promote best practices through industry accountability programs and safe harbors. The government can also advance the goals of this RFC by incentivizing and funding research and promoting open source frameworks.

E. Avoiding Missteps.

The RFC has recognized that recent actions by foreign countries and States have led to a "fragmented regulatory landscape" regarding consumer data privacy.[34] Europe's GDPR has sought to codify privacy and data protection principles, but some details of the policy have shown a lack of clarity that can hurt startups and small businesses seeking to enter the marketplace.[35] For example, academics Peter Swire and Yianni Lagos noted the tension between

[34] RFC at 48600.
[35] *See* Jia & Wagman, *supra* note 13.

moving data between services and users' security interests in evaluating an early version of the GDPR's right to data portability.[36] In contrast to the GDPR, U.S. policymakers should provide clear definitions and clarity to individuals and organizations that handle data so individuals are assured that their data is protected and handled responsibly. For example, a national standard should protect individuals and their personal information through clear notifications, and it should define a harm-based trigger for notification while also allowing organizations flexibility to find the most effective means of notifying individuals.

F. Next Steps and Measures for the Administration.

1. Achieving U.S. Leadership: Continued Support of Privacy Shield and Engagement in International Fora.

The EU-U.S. Privacy Shield Framework is critical to transatlantic information flows, driving $260 billion. As Secretary Ross has stated, "Privacy Shield works."[37] Thousands of small and medium-sized companies rely on Privacy Shield to transfer personal data from the European Union to the United States while ensuring adequate protection of European citizens' data. Privacy Shield has enhanced privacy safeguards and provided legal clarity for certified companies and users. The agreement's multi-layered privacy protections are based on a wide range of constitutional, statutory, administrative, and non-judicial protections and remedies available in the U.S. to ensure adequacy under EU law, including several commitments by federal agencies, law enforcement, and the U.S. intelligence community. CCIA is pleased with

[36] Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335 (2013), https://pdfs.semanticscholar.org/b826/c58ff279d3e6b3ae96583dcd5f023585b68b.pdf.

[37] Wilbur Ross, Op-Ed: Transatlantic Privacy Deal is Vital to Trade (Oct. 18, 2018), https://www.commerce.gov/news/opinion-editorials/2018/10/op-ed-transatlantic-privacy-deal-vital-trade.

the recent, second annual EU-U.S. Privacy Shield review[38] and encourages NTIA and the Administration to continue their strong efforts to support Privacy Shield.

In addition, CCIA encourages NTIA and the Administration to continue working with other international fora to identify practices that have proved effective at ensuring privacy protections and developing policies where appropriate. Indeed, by adopting baseline, Federal privacy legislation, the U.S. would be in a stronger position when negotiating international agreements with the EU and other countries. The U.S. would also be able to provide a substantive alternative to recent extraterritorial regulations with problematic provisions, like the GDPR.

2. Continue Multi-Stakeholder Dialogues.

NTIA and the Executive Branch should continue the conversations that have begun with this RFC. Multi-stakeholder engagement can help with the development of codes of conduct that can be enforced by the FTC. Technology continues to advance at a breakneck pace, so it is critical that policymakers consult with industry, academics, the technical community, and civil society when assessing whether elements of a privacy framework are feasible and commercially viable.

IV. Definitions.

CCIA submits the following in response to the NTIA's requested input regarding relevant definitions.

Personal Information or Data: Personal information or data includes any data under the control of a covered organization, that is not de-identified or otherwise generally available to the

[38] Joint Press Statement from Commissioner Věra Jourová and Secretary of Commerce Wilbur Ross on the Second Annual EU-U.S. Privacy Shield Review (Oct. 19, 2018), https://www.commerce.gov/news/press-releases/2018/10/joint-press-statement-commissioner-vera-jourova-and-secretary-commerce.

public through lawful means, and is linked or practically linkable to a specific individual, or linked to a specific device or account that is associated with or routinely used by an individual.

An overly broad definition of "personal information" may go beyond information that actually identifies a person to include any information that could be linked with a person, which arguably includes all information. A definition such as this would not only be confusing and difficult for compliance, but it also could actually undermine important privacy-protective practices like encouraging organizations to handle data in a way that is not directly linked to an individual's identity.

Different types of personal data can vary in sensitivity, depending on the context. However, some personal data is almost always sensitive. This includes data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation, and certain data of known minors.

Privacy Risk: The potential for personal information, on its own or when linked to other information that might identify an individual, to cause economic loss, discrimination, exclusion, loss of self determination or physical, reputational, or professional harm to an individual.

Covered Organizations or Entities: Covered organizations or entities include all organizations that process personal information, regardless of whether they have a direct or commercial relationship with an individual whose information they hold.

Proportionality: Reasonable data protection practices may differ across covered organizations. Context, including an organization's scale and resources, the sensitivity of the data it holds, and its uses for that data, should inform the measures that it puts in place to protect data.

V. Conclusion.

CCIA applauds NTIA and the Commerce Department for conducting this public comment process. CCIA encourages NTIA and the Commerce Department to continue pursuing a constructive dialogue, as well as broad engagement and input from stakeholders and the public, to advance consumer privacy while protecting prosperity and innovation. Recent controversies have shifted public attention to how data is collected and used online, but sudden action by the U.S. government could adversely impact innovation for online services and privacy controls, leading to stark choices by small and new firms. However, CCIA hopes that through this public comment process, policymakers will gain more information from stakeholders and the public, and that policy outcomes will: (1) aim to protect data through a robust, technology-neutral framework for assessing and managing privacy risks to individuals and organizations; and (2) seek to promote innovation in both digital services and privacy protection.

November 7, 2018

Respectfully submitted,

/s/ John A. Howes, Jr.
Policy Counsel
Jacqueline Yin
Legal Fellow
Computer & Communications Industry Association (CCIA)
655 15th Street, NW Suite 410
Washington, DC 20005
(202) 783-0070
jhowes@ccianet.org

Computer & Communications
Industry Association
Tech Advocacy Since 1972

PRIVACY PRINCIPLES:

A New Framework for Protecting Data and Promoting Innovation

Purpose

As the world becomes increasingly data-focused, attention has inevitably shifted to the impact of data on consumers and whether and how improvements should be made. Recent controversies have shifted how companies and consumers think about how data is collected and used online, generating some positive responses in terms of practice and transparency. It is important for the U.S. to have a healthy data ecosystem with transparency and accountability, which will help drive innovation and U.S. competitiveness.

CCIA supports the development of baseline, Federal privacy legislation that would ensure that data is handled responsibly and with transparency while also ensuring that individuals can benefit from innovation and new technologies. Such a framework should be technology-neutral, meaning it should not provide specific technology mandates; sector-neutral, meaning it should apply to online and offline organizations; and it should provide for safe harbors and flexibility for organizations to make adjustments according to the needs of individuals and evolving technology. CCIA presents these "Privacy Principles" to help guide the development of a national policy on consumer privacy.

Policy Overview

These principles aim to protect data through a robust, technology-neutral framework for assessing and managing privacy risks to individuals and organizations, and to promote innovation, in both digital services and privacy protection. Organizations across the digital ecosystem use personal data to provide innovative services. Responsible data use can be beneficial for people, businesses, and society. Reasonable data protection measures that align with individuals' expectations can protect people and communities from harms that result from misuse of data and help maintain the trust that enables the digital economy.

When evaluating the reasonability of an organization's data protection practices, it is important to understand the context in which an organization collects, processes, and uses personal information. This context can include the nature of the relationship between an individual and the organization; the potential benefits an individual, organization, and society might receive from particular uses of information; and individuals' expectations regarding data protection.

Individuals depend on organizations to use their data responsibly and be transparent about what they are collecting and how they are collecting and using it. Therefore, organizations must respect individuals' interests when they process personal information. Organizations should make reasonable best efforts to account for and mitigate potential harms to individuals, communities, and society.

Scope and Definitions

Personal information or data include any data under the control of a covered organization, that is not de-identified or otherwise generally available to the public through lawful means, and is linked or practically linkable to a specific individual, or linked to a specific device or account that is associated with or routinely used by an individual.

Different types of personal data can vary in sensitivity, depending on the context. However, some personal data is almost always sensitive. This includes data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation, and certain data of known minors.

Privacy risk
The potential for personal information, on its own or when linked to other information that might identify an individual, to cause economic loss, discrimination, exclusion, loss of self determination, or physical, reputational, or professional harm to an individual.

Covered organizations or entities include all organizations that process personal information regardless of whether they have a direct or commercial relationship with an individual whose information they hold.

Proportionality
Reasonable data protection practices may differ across covered organizations. Context, including an organization's scale and resources, the sensitivity of the data it holds, and its uses for that data, should inform the measures that it puts in place to protect data.

CCIA | 655 15th St NW #410 | Washington, DC 20005 | ccianet.org | Phone: +1 (202) 783-0070 | Fax: +1 (202) 783-0534

Interoperability
Cross-border data flows are essential to the modern economy. Organizations and individuals benefit from consistent compliance programs based on widely shared principles of data protection. These principles are intended to be interoperable and consistent with existing cross-border data transfer mechanisms, industry standards, and other cross-organization cooperation mechanisms.

Requirements for Organizations

Control
Covered organizations must provide appropriate mechanisms for individual control, considering the service. Individuals should be able to object to data processing where it is feasible, but specific consent should not be mandatory for every aspect of data processing, which could create an overly complex and confusing experience for the individual and divert from the overall goals that the policy seeks to achieve. Policymakers should also keep in mind that the responsible processing of personal information is necessary to simply operate some services.

Access
Individuals must be able to access the personal information that they have provided to a covered organization, and it should be made available for export in a machine-readable format.

Accuracy
Personal information should be accurate, current, and complete to the extent possible for the purpose for which the covered organization maintains the data.

Deletion
Pursuant to the above "Access" principle, covered organizations should afford users with the ability to correct and/or delete the data that they provide to that organization when it would be practical and provided that deletion would not implicate the personal information of others.

Portability
Covered organizations should make reasonable efforts to enable authenticated users to obtain data they provide to that organization for their own purposes or for use with a different organization or service, provided that these data portability tools do not implicate the personal information of others. Data transfers between covered organizations should be private, secure, and balanced. Data portability tools should: (1) allow users to download and move data they have provided to the service, but not data that may relate to other users; (2) afford users control over how and when the tools are used; and (3) be tailored to the privacy and security expectations of specific products and services. Further, data portability tools should enable machine-to-machine transfers where technically feasible.

CCIA | 655 15th St NW #410 | Washington, DC 20005 | ccianet.org | Phone: +1 (202) 783-0070 | Fax: +1 (202) 783-0534

Security and Integrity
Users should expect that organizations handling their data will do so carefully and responsibly with reasonable measures to protect personal information from unauthorized access, misuse, modification, disclosure, loss, and destruction. Policy should account for and be proportionate to the risk of harm. Organizations should follow consensus best practices, and if a security breach occurs, organizations should notify individuals expeditiously when there is a significant risk of harm.

Onward Transfers
Covered organizations should ensure that personal information that they collect or process is protected in a manner consistent with the above principles even if it is transferred to third parties. Covered organizations should use enforceable mechanisms and independent audits to ensure that third parties protect data according to these principles.

Accountability

Transparency
Covered organizations must be transparent about the types of personal information that they are collecting and how they are collecting and using it. Covered organizations should be clear about whether the personal information may be transferred to third parties, how long information may be retained, and what choices and controls individuals have with respect to their personal information. Covered organizations should make reasonable efforts to actively inform individuals, making the information relevant and actionable, about data use in the context of the relevant services.

Accountability
Covered organizations should be held accountable for meeting the requirements set out in these Privacy Principles. Covered organizations should regularly assess the privacy risks associated with their collection, processing, and use of personal information; develop systems to mitigate risks in a reasonable and proportionate manner; and monitor services for bias and disparate impacts. Organizations should practice privacy by design, building products and services that prioritize privacy, security, reliability, and reduce the likelihood of vulnerabilities, which will help earn user trust. Policymakers should set baseline requirements but enable flexibility to meet those requirements and promote industry accountability programs and safe harbors.

Enforcement
A robust federal baseline would provide clear standards for covered organizations and ensure that individuals across the United States can expect consistent data protections from organizations that retain their data. A national, privacy framework should be consistent throughout the United States, so state laws concerning data privacy, security, and breach notifications should be preempted where appropriate. This framework should be enforced primarily by the FTC at the federal level, but it should allow for enforcement by state attorneys general where the FTC has declined to act.

CCIA | 655 15th St NW #410 | Washington, DC 20005 | ccianet.org | Phone: +1 (202) 783-0070 | Fax: +1 (202) 783-0534