ASSOCIATION OF RESEARCH LIBRARIES

Developing the Administration's Approach to Consumer Privacy

National Telecommunications and Information Administration
Docket No. 180821780-8780-01

ARL supports strong privacy protections for users, with the understanding that these laws should be clear and avoid overly-prescriptive requirements that make compliance difficult. Policymakers should avoid rules that require high costs for compliance, which can disadvantage non-profit institutions and start-up companies. In considering privacy regulations, the Department should convene individuals and organizations to explore these issues and any convening should include not only voices from the private sector, but also public institutions, and consumer advocates. Libraries have long advocated for user privacy, balanced against new digital capabilities and related issues to simultaneously promote user experience, and would welcome the opportunity to participate in these proceedings.

The RFC raises a number of important questions regarding consumer privacy, the scope of regulations and expectations. Several elements of privacy law, such as ensuring transparency and consent, are so critical that they must be included for regulations to be meaningful and effective. Other areas require deep consideration, because of the nuanced issues and potential unintended consequences of laws that either sweep to broadly in its protections, or do not extend far enough.

From the outset, regulations should encourage companies and services to consider privacy implications before any data is collected, to avoid the overly-inclusive approach to collection. Ensuring that privacy is included in the design of services and is the default position would encourage the collection and storage of only the necessary data. While many companies today collect vast swaths of data and later find different uses for such data, regulations should be designed to shift this approach to minimize data collection. Certainly, if other uses for the data are found in the future, services would be free to request consent from its users.

Strong Transparency and Consent Requirements Are Key Features for Meaningful Privacy Regulation

Transparency is an essential hallmark for any privacy law, allowing users to read and understand the terms under which they allow their data to be collected and used. Policies must be easily accessible at the time the user engages with the service. Users should understand what information is collected, stored, used and shared from the outset. Transparency must mean more than mere notice or simple access to terms and conditions; the language use must be plainly written for the target audience and stripped of any legalese. These measures should also consider inclusion of privacy support, allowing users to ask questions or have privacy options explained.

In tandem with transparency, clear consent must be required before the collection of any data. Meaningful consent is impossible unless the user can truly understand what policies and data

collection practices exist. Strong consent rules would not only require affirmative consent, but also consider opt-in as the default position, rather than allowing users to opt-out. In an opt-in system, users would have the opportunity to make a clear choice to allow collection from the outset rather than needing to go through various steps to prevent data collection. ARL agrees with the NTIA's statement in its Request for Comment that "relying on user intervention may be insufficient to manage privacy risks" and the typical notice-and-consent systems used in the technology industry today is insufficient. Furthermore, using or applying data for purposes other than the ones explicitly agreed to should presumptively violate privacy regulations.

Additionally, any regulations should make clear that consent given once does not mean consent is given forever. Users must be allowed to withdraw consent at any time.

Should a user withdraw his consent or choose to move to a different platform or service, the user should be permitted to take the data collected about him. Data portability is essential in promoting competition and user choice. Without data portability, users will be locked into existing or more prominent platforms and new entrants to the market will be at a serious disadvantage, stifling innovation.

Additionally, all users should have access to the same level of protections regardless of resources. Privacy regulations must ensure that any processes the user engages in—for example, withdrawing consent or requesting their personal data—are easy to use, avoiding a digital divide in which only those with adequate resources can make use of these features.

Combining strong transparency requirements, meaningful consent and data portability empowers the user to make educated choices regarding how he or she shares personal data.

Right to Be Informed of Security Breaches

Additionally, the Request for Comment raises the issue of security safeguards to secure personally identifiable information on data. Just as users must be able to understand the collection policies, so too must they be informed when their data has been breached. Regulations should incorporate appropriate notification standards for security breaches.

Meaningful Oversight and Remedies Are Necessary to Ensure Privacy Compliance

For regulations of any kind to be effective, meaningful oversight and penalties for failure to comply must be included. The Federal Trade Commission (FTC) is already well-equipped to handle consumer complaints and would be the logical agency to enforce privacy regulations. However, the FTC must have greater enforcement authority, including the ability to impose meaningful fines from companies who fail to comply with privacy standards. The FTC's current jurisdiction over privacy issues is limited and has proven to have little effect on data collection practices in major technology companies.

Right to Deletion Raises Complex Issues Requiring Careful Consideration and Nuanced Approach

The Request for Comment discusses the right to rectify, complete, amend or delete data, which must involve a delicate balance between consumer privacy, freedom of expression and the importance of preserving the historical and cultural record. In the European Union, users have a broad right to request deletion, including for information that is deemed as not "relevant." Such

an expansive approach raises serious concerns, including difficulties in determining what is relevant. Libraries have long been strong advocates of the First Amendment, and if the right to delete data sweeps too broadly, a right to deletion could be used to silence critics. Libraries also have a central mission of preserving and providing access to information; allowing the right to deletion will skew the historical record, make information more difficult to find and impair preservation efforts. Changes to the public, historical record—which includes searchability on the Internet—can fundamentally skew research results and efforts to analyze statistical data. Any regulations that would have an effect on altering the historical record also raises serious ethical questions. At a minimum, any regulations that provide a right to deletion must include a carveout for public information and records. As with any regulation, unintended consequences and potentials for chilling effects must also be carefully considered. With respect to the right to be forgotten, critics have observed that intermediaries may err on the side of delinking or delisting results to ensure compliance, without appropriately balancing the right to freedom of speech.

Incentivizing Privacy Research and Development of New Models

Privacy regulations must strike a delicate balance between protecting consumers while also avoiding unduly burdensome regulations that could stifle innovation. In order to enhance protections while simultaneously exploring new innovations and models, the federal government should incentivize privacy research. Such research can identify not only security flaws, but also develop new models and tools that may enhance privacy outcomes.

ARL supports the creation of strong federal privacy regulations. While some elements of meaningful privacy rules are clear, such as transparency and consent, other areas require thorough consideration and a nuanced approach. Privacy regulations should protect users and provide incentives for compliance, yet avoid overly-burdensome requirements that would stifle innovation.