
UNITED STATES COUNCIL FOR INTERNATIONAL BUSINESS

USCIB COMMENTS ON FTC PRELIMARY STAFF REPORT PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE – A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS

The United States Council for International Business (USCIB) commends the FTC for the consultative process it held on privacy last year as an input to developing the Preliminary Staff Report for Protecting Consumer Privacy in an Era of Rapid Change – a Proposed Framework for Businesses and Policymakers ("Proposed Framework"). We look forward to participating in further discussion on the Proposed Framework, one that seeks to achieve effective enforcement of privacy and narrowly tailored and essential public policy objectives. The Proposed Framework should not create undue burdens, unintended consequences or constraints on innovation and should support the potential economic and societal benefits of new technologies and business models.

**Scope:**

Privacy law and policies in the United States have had a long tradition of seeking to protect individuals from undesired intrusions into their private lives. We commend the FTC for its innovative thinking and for probing whether privacy law ought to be expanded to cover information that is not actually linked to an individual, but may be potentially linkable to an individual or their computers or devices. We caution, however, that this is a major shift in United States privacy law and a new paradigm that should not be undertaken lightly. Eliminating any distinction between personal and non-personal data in all circumstances is unnecessary. Doing so will create enormous difficulties, affecting day to day operations for many businesses, and may in fact be inconsistent with existing legal frameworks which recognize such a distinction.

Where businesses do not link the data they collect to data which would identify individuals, we question the policy goal that would be achieved by subjecting such potentially "linkable" data to the entire panoply of the FTC's Proposed Framework. Indeed, including potentially linkable data in the framework may have the adverse effect of requiring businesses to collect more data about individuals in order to guarantee that the individuals are provided with effective notice, choice, and access, despite that lack of actual practice of linkage We also support the continued ability of businesses to use aggregated or anonymized data and urge the FTC to help ensure that data that is not considered personally identifiable information when collected would not become so when placed into another context which ensures anonymity. We therefore disagree with the blanket inclusion of potentially linkable data into the proposed framework.

**Privacy By Design**

We are supportive of the concept of privacy-by-design. Indeed, businesses today are already developing and implementing risk assessment processes, such as privacy reviews as well as more informal internal controls, and we stress the need to apply both tools and concepts in a flexible manner. These processes need to be flexible so that organizations can effectively address privacy concerns while recognizing infrastructure, physical, human, scale and technical aspects, and taking into account the use and nature of information.

The FTC should avoid attempting to create or promote a structure that involves mandatory compliance with detailed standards, or mandatory third party detailed product reviews; this would not only decrease time to market and increase product costs, but will freeze technology and adversely affect innovation in privacy and security-enhancing technologies and practices. We should also note that apart from general flexibility in order to accommodate different operational environments, any new framework should need also reflect varying sectoral concerns, for example, existing sector and media-specific legal provisions and requirements; in addition, such frameworks should reflect technology, platform and business model neutrality

**Improved Choice/Do Not Track**

The FTC Framework correctly identifies that there are a number of uses of data or business processes that are either obvious or expected by consumers, including, among others: fulfillment, customer support, use of service providers, fraud assurance, security, operational aspects of providing the requested services as well as other every-day business purposes. We believe that "commonly accepted practices" should be defined as broadly as possible. The Framework highlights that these expected processes and uses should not be the subject of consent, and would enable consumers to better focus on important choices that may relate to unexpected uses of information. The "informed and meaningful choice" that must be offered with respect to practices that are not deemed to be commonly accepted should be provided via an opt-out, as opposed to an opt-in.

Business favors approaches that streamline notice and create less complexity, thereby providing greater clarity to users as well as more effective choices. However, we are concerned that the Framework oversimplifies the necessary scope of these commonly accepted uses and practices. As currently described, the scope of "commonly accepted practices" is not sufficiently broad. It is essential, for example, that commonly-accepted practices be defined in a manner consistent with existing laws, and encompass threats to persons or property (both physical and intellectual) that may fall short of "fraud." As a consequence of this unduly narrow list, the proposed framework could impose significant constraints on the U.S. economy by posing unnecessary business and operational issues for many industries and business models. In addition, the FTC should not overly constrain the needed flexibility of operations or the application of new technologies and business models. We reiterate that any privacy framework should be technology,

platform and business model neutral, and flexible enough to allow for the inevitable and fast-paced changes in technology.

We believe that 'Do Not Track' must be the subject of further inquiry and discussion; we ask the FTC to recognize the important progress industry self-regulation is making on offering notice and choice in the online behavioral advertising (OBA) context. The complexity and applicability of a 'Do Not Track' proposal is far from straightforward and needs further consideration of legal, practical and operational impediments, and whether other solutions are becoming available. We also believe that no single solution will be appropriate in all cases, so consideration should also be given to different ways in which these objectives can be achieved.

## Transparency

The general principle of transparency may lend itself to a variety of interpretations. While we support the need for improved transparency where confusion may exist, we are concerned that some efforts to provide granular information related to complex processes may actually have a contrary effect. Individuals need useful information, not vast amounts of information. Too much information may improperly burden the data subject in terms of both volume and the technical nature of the information. To that end, we support the use of plain language in lieu of detailed language to meet legal requirements in privacy notices. However, such plain language should be recognized as meeting such legal requirements. There is clearly no single approach to ensuring transparency, and effective, creative approaches should not be constrained by prescriptive laws

## Reasonable Access

We believe that the FTC should recognize that there is both cost and complexity associated with reasonable access and that the FTC should consider the burden of providing such access.

Where access is provided, reasonable costs should be able to be recovered from the requester. There are also often business needs to retain information in a personally identifiable form, such as information related to quality or safety complaints. Access and correction goals cannot be implemented in a manner that subverts the ability of companies to take reasonable steps to minimize potential liability, or to utilize data to improve products and services.

## Education

The need for education and awareness-raising has been and remains a shared objective across stakeholders. Providing notice to an individual who has an understanding of privacy is much more effective. The Framework highlights the need for industry

education efforts. We would suggest that the education be the subject of a public-private partnership. Unfortunately, some education efforts by individual companies may be misunderstood as being self-serving if not coordinated with a broader government message. We would, therefore, like to engage in further consultations on how such a partnership approach might be progressed towards this shared objective.