ISACA
1700 E. Golf Road, Suite 400
Schaumburg, Illinois 60173, USA
Telephone: +1.847.253.1545
isaca.org | E-mail: info@isaca.org

ISACA Response to Request for Comments on NTIA Notice on Developing the Administration's Approach to Consumer Privacy

Document: 83 FR 48600
Document Number: 2018-20941
Agency/Docket Number: 180821780-8780-01

ISACA, on behalf of its nearly 60,000 information and cyber security professionals in the United States and its global community of nearly 140,000 professionals, is grateful for the opportunity to provide comments on the National Telecommunications and Information Administration's (NTIA's) Notice on Developing the Administration's Approach to Consumer Privacy.

The Notice on Developing the Administration's Approach to Consumer Privacy is both timely and welcome. While the strategic aims of the Notice are well-crafted, there are several elements that ISACA believes deserve additional consideration and potential action:

II. Request for Comment

A. Through this RFC, the Department is first seeking feedback on what it believes are the core privacy outcomes that consumers can expect from organizations.

1. Are there other outcomes that should be included, or outcomes that should be expanded upon as separate items?

2. Are the descriptions clear? Beyond clarity, are there any issues raised by how any of the outcomes are described?

3. Are there any risks that accompany the list of outcomes, or the general approach taken in the list of outcomes?

There were a number of items in Department's approach to consumer privacy that ISACA believes are of merit, and we commend the Department for choosing to include them. However, it is ISACA's considered opinion that this approach, as currently outlined, misses some additional opportunities for success.

Within Section A, subsection 1, there are two key elements ISACA believes are missing: time limits for the length of time data will be kept, and an insistence on language within the privacy program that is clear and understandable to consumers at levels age- and education-appropriate. Short, plain non-legal language would be best suited to the task. Also, ISACA believes that "should" in the final sentence leaves effective transparency as an option for organizations; ISACA feels that the mandate inherent in changing "should" to "must" in that sentence is more effective in supporting the Department's consumer protection efforts. As for

the time limits on data retention, the inclusion of language similar to "*when data is no longer legally required, then such data will be securely deleted*" would do a great deal to address time limits on the holding of private data.

Within Section A, subsection 2, the emphasis on control is written from the perspective of the organization, not the consumer, and ISACA believes this to be an ill-advised approach. Inserting language along the lines of "users' rights shall be made available at the time of collection" would go a long way towards writing this section from the perspective of the consumer.

Within Section A, subsection 3, ISACA believes that the concluding sentence (*Other means of reducing the risk of privacy harm [e.g. additional security safeguards or privacy enhancing techniques] can help reduce the need for such minimization.*) should be eliminated. The use of "safeguards" or "privacy enhancing techniques" should not exempt companies from data minimization; this subsection protects enterprises, not the individuals whose data those enterprises use. It is ISACA's considered opinion that a balance must be struck that protects the data of the individual, but still enables enterprises to innovate—but the success of one cannot occur at the expense of the other.

Section A, subsection 4 also contains elements regarding security which, in ISACA's considered opinion, require refinement. This subsection discusses "*security measures appropriate to the level of risk associated with the improper loss…of personal data*." A more consumer-focused approach, ISACA believes, would be to include language along the lines of "*security measures commensurate with the risk to the user/individual if such data is exposed*." Likewise, the inclusion of secure deletion as part of securing data at all stages—as outlined in the final sentence of subsection 4—would also be beneficial in giving primacy to the protection of the consumer.

Within Section A, subsection 5, "*qualified access to personal data they have provided*" seems to place delimiters on the access, rather than the verification of the user as being the individual whom they say they are. ISACA believes that such verification is essential but placing limitations on access once a user has been verified is not advisable; it is, after all, the user's data, ultimately.

Accountability is also a concern for ISACA. Within Section A, subsection 7, it states: *Organizations that control personal data should also take steps to ensure that their third-party vendors and servicers are accountable for their use, storage, processing, and sharing of that data*. While ISACA agrees in principle with what is expressed, we believe it lacks both specificity and teeth. Additionally, the subsection states that organizations "should" take steps to ensure accountability from third-party vendors. "Should" is not "must", and ISACA believes this to be a missed opportunity to introduce more stringent accountability throughout the vendor and servicer community, thereby strengthening the overall digital ecosystem. It would also be of benefit, ISACA believes, for the Department to consider defining accountability for compliance as well. In this regard, the creation of a Data Protection Officer, or a similar professional dedicated to ensuring compliance requirements were met and that enterprises are accountable, would also be advisable for consideration.

Also, within subsection 7 is the term "privacy-by-design". However, the term is not defined anywhere within this document. Much of the language associated with the foundational principles of privacy-by-design—*proactive, preventative, lifecycle, breach, consent, default*—is absent anywhere within this draft document. Defining privacy-by-design, particularly utilizing terms in keeping with the principles underpinning privacy-by-design would, ISACA believes, be of benefit to the Department's consumer privacy efforts.

It is also important to note what is not contained in Section A: availability. This is a requirement within the GDPR, and it would benefit America's digital economy to include it as a principle and outcome here, in ISACA's considered opinion.

Overall, in ISACA's considered opinion, while a risk-based approach is appropriate, there is danger that surrounds this sort of an approach. Questions of organizational culture and risk must be addressed, as should issues of compliance. Additionally, ISACA believes the general approach taken in the list of outcomes could also benefit from a requirement to report, as well as repercussions (i.e., fines, etc.) for non-compliance. At present, there are various pieces of legislation that require both annual privacy reporting and compliance to data privacy rules at the risk of fines or incarceration, and ISACA believes the Department's actions should also take such measures into consideration, moving forward.

B. The Department is also seeking feedback on the proposed high-level goals for an end-state for U.S. consumer-privacy protections.

1. Are there other goals that should be included, or outcomes that should be expanded upon?

2. Are the descriptions clear? Beyond clarity, are there any issues raised by how the issues are described?

3. Are there any risks that accompany the list of goals, or the general approach taken by the Department?

In Section B, *High-Level Goals for Federal Action*, subsections 1 and 3 takes some excellent strides forward but could bear some improvement. Both subsections, in different ways, appear to demonstrate the Department's goal of an integrated, comprehensive regulatory, statutory and public policy approach to consumer protection, and ISACA is in complete agreement with the Department's goals.

We are already seeing the beginnings of a regulatory 'patchwork quilt' developing; absent overarching national legislation, State jurisdictions have already begun to address issues of consumer privacy. It is imperative, ISACA believes, that a unified approach to consumer privacy be taken at the Federal level, one which unifies the Federal government's approach to privacy, as well as the rest of the United States' public and private sectors' approaches and includes appropriate data subjects' rights.

The European Union's General Data Protection Regulation (GDPR) sets a baseline to which the Union's nations must conform, at a minimum. It is up to individual nations to then decide if they wish to establish stronger protections (e.g., Germany). ISACA strongly believes a GDPR-like approach, with the Federal government creating legislative baselines that States can adhere to or enhance through their respective legislative efforts is a more balanced and ultimately more harmonious solution.

It should also be noticed that subsection 3's focus, however, is on organizations protecting individuals and not on the ability for individuals to protect themselves. Another of the key precepts of the GDPR is that the data privacy and protection measures outlined in the GDPR travel with the individual, regardless of location—and that the GDPR applied to all EU residents. It is in this focus on the individual where ISACA believes the Department is missing an opportunity for success that is easily addressed by including similar concepts in consumer privacy efforts, applicable to all US residents, going forward.

ISACA would also suggest that in subsection 2, “collaboration” should be the driving focus, not “compromise”.

Within Section B, subsection 6, the goal of incentivizing privacy research requires far more detail than what is put forth in this subsection, and ISACA hopes to see that detail in future drafts of this document. In its present state, this subsection puts no limits on what government support of privacy research could bring with it as a requirement (i.e., security ‘back doors’, etc.). ISACA believes this section, to best benefit the consumer, deserves either additional clarity, or extensive amendment to include funding and research support systems developed separate and apart from government.

The question of utilizing the FTC as the appropriate Federal agency to enforce consumer privacy that is raised in Section B, subsection 7 is also a matter of concern for ISACA. The exceptions raised within that subsection for sectoral laws outside FTC authority (i.e., HIPAA) seem to point towards alternatives, such as creating a Federal agency that could ensure consumer privacy protection across all sectors, an agency unbound by potential conflicts of interest or lack of jurisdiction. ISACA believes that, while creating such an organization might bring with it challenges of its own, it is likely to be a more efficient and effective solution.

Within Section B, subsection 8, the issues of scalability that are raised are also, in ISACA’s considered opinion, somewhat off the mark. Today’s digital marketplace is not a series of discrete transactional encounters; it is an interconnected ecosystem and strengthening consumer privacy protections in even the smallest of enterprises benefits all within that ecosystem. While the Department does not wish to make small businesses the primary target of privacy-enforcement activity, ISACA believes this is an ill-advised choice. Likewise, the distinction made in this subsection between third-party data processing vendors and organizations that control data is also, in ISACA’s considered opinion, a less-than-optimal approach. The same level of protections must be present for the consumer, regardless of what enterprise is interacting with their data. Subsection 8, in ISACA’s view, could also benefit from a focus on the need to include appropriate risk assessments and controls as a critical component of scalability.

C. The Department is seeking comments that describe what the next steps and measures the Administration should take to effectuate the previously discussed user-centric privacy outcomes, and to achieve an end-state in line with the high-level goals. In particular:

1. Are there any aspects of this approach that could be implemented or enhanced through Executive action, for example, through procurement? Are there any non-regulatory actions that could be undertaken? If so, what actions should the Executive branch take?

2. Should the Department convene people and organizations to further explore additional commercial data privacy-related issues? If so, what is the recommended focus and desired outcomes?

3. What aspects of the Department's proposed approach to consumer privacy, if any, are best achieved via other means? Are there any recommended statutory changes?

ISACA commends the Department’s efforts thus far and would suggest that its next steps include the convening of public and private sector representatives into collaborative teams to explore additional consumer

and data privacy issues. Additionally, similar collaborative teams could engage in efforts to explore statutory changes to increase consumer privacy. Ideally, these two sets of teams could function as two halves of a larger, consensus body, convened as a whole to address regulatory, statutory, non-regulatory and other actions that may need to be examined in order to best ensure consumer privacy.

D. The Department understands that some of the most important work in establishing privacy protections lies within the definitions of key terms and seeks comments on the definitions. In particular:

1. Do any terms used in this document require more precise definitions?

2. Are there suggestions on how to better define these terms?

3. Are there other terms that would benefit from more precise definitions?

4. What should those definitions be?

Throughout our response, ISACA has indicated instances in which the Department's terminology could be edited or amended (i.e., the use of "collaborate" rather than "compromise" in Section B, subsection 2, etc.). The definition of key terms in establish privacy protections is of paramount importance, which is why ISACA believes that defining of those terms is a task best approached collaboratively, similar to the approach our organization has suggest for addressing any statutory or other changes to support consumer protection. This is the best way, ISACA believes, to arrive at definitions that are robust and able to provide a solid underpinning for comprehensive and responsive privacy protections.

E. One of the high-level end-state goals is for the FTC to continue as the Federal consumer privacy enforcement agency, outside of sectoral exceptions beyond the FTC's jurisdiction. In order to achieve the goals laid out in this RFC, would changes need to be made with regard to the FTC's resources, processes, and/or statutory authority?

As was stated earlier in our comments on Section B, subsection 7, ISACA believes the FTC may not be the best vehicle for this work. The exceptions raised regarding sectoral exceptions outside FTC authority (i.e., HIPAA) suggest that an alternative organization might be better suited to this task. Creating a Federal agency that could ensure consumer privacy protection across all sectors, an agency unbound by potential conflicts of interest or lack of jurisdiction could be a more effective solution, in ISACA's considered opinion.

F. If all or some of the outcomes or high-level goals described in this RFC were replicated by other countries, do you believe it would be easier for U.S. companies to provide goods and services in those countries?

If the outcomes and high-level goals in this RFC are in alignment with existing data privacy measures, such as the European Union's GDPR, this could result in additional nations aligning their data privacy measures with either or both constructs. It would depend, however, upon how aligned these data privacy measures were, before their impact upon other nations could be ascertained.

However, it is imperative, if the goal is for U.S. goods and services to be provided to a wider swath of countries, that an environment be created in which mutual levels of concern for data privacy exist. In efforts to support the outcomes and high-level goals described by the Department, ISACA believes there are certain elements that require inclusion, among them:

- The appointment of data protection officers (or similar professionals) to monitor and oversee data processing activities, to better ensure accountability for compliance.
- The existence of data registries to support data inventory and mapping, so that enterprises can ascertain exactly what data is collected and retained, where that data is stored, how that data will be secured, and how it will be used.
- The gap analysis of data privacy efforts, so that an enterprise's internal efforts can be compared to the appropriate statutory, regulatory, or other requirements.
- Based upon the results of an enterprise's gap analysis, the creation of a compliance prioritization and action plan that addresses any risks—major and minor—identified during the analysis.
- Appropriate industry standard data security measures including, but not limited to, data protection anonymization, encryption, data lifecycle management and data retention limitations.
- The thorough documentation of data privacy and security policy processes, as well as the documentation of any security or privacy issues that arise during the course of business.
- A lawful basis for processing personal data must be present and must include the obtaining and management of consent from individuals for the appropriate use of their data.
- Transparency of activities must be a primary consideration; individuals should be provided with plain-language privacy notices that clearly delineate the individual's rights, as well as the enterprise's data privacy practices.
- Should a data breach occur, timely notification to affected users and the appropriate data authorities must occur as well.

G. Are there other ways to achieve U.S. leadership that are not included in this RFC, or any outcomes or high-level goals in this document that would be detrimental to achieving the goal of achieving U.S. leadership?

In an earlier response, ISACA suggested the word "collaborate", rather than "compromise"; one is indicative of partnership, the other of negotiation. ISACA strongly believes that leadership is at its strongest when it works collaboratively to accomplish its goals, holding steadfast to its principles, yet working together to find common

ground. The quest for sound data privacy measures and strong consumer protection efforts is no different and should be approached in a collaborative matter to ensure the highest chances for and levels of success.

Thank you again for this opportunity to share ISACA's perspectives on the National Telecommunications and Information Administration's Notice on Developing the Administration's Approach to Consumer Privacy. ISACA looks forward to continuing to work with the Department and the Federal government on consumer privacy issues and concerns in the years ahead.