

Written Comment on the National Telecommunications and Information Administration, U.S. Department of Commerce’s Notice, “Developing the Administration’s Approach to Consumer Privacy” – Docket No. 180821780-8780-01

In response to Question A2 (Are the descriptions clear? Beyond clarity, are there any issues raised by how any of the outcomes are described?)

The following four paragraphs will refer to the following quotation featured in section A2 (“Control”) of the document:

“Users should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide to organizations.”

The “Control” section and in particular this sentence indirectly comment on an underlying challenge inherent to supporting consumer privacy. This challenge is manifest in that the technological service providers in question have business models that rely upon collected users’ data in order to provide services to consumers. At the same time, the services that they provide are now integral to participation in civic life in the U.S.¹ As an arbiter of both profit-generating activities and civic activities, technology companies toe a new and challenging line: how to enable access to civic participation while at the same time generating profit?

In order to avoid infringing upon consumer privacy by reducing the amount of behavioral data they collect about consumers, some technology companies – in particular digital media providers – have opted for subscription-based business models or fee-for-service business models.² These approaches, though reasonable attempts to mitigate privacy concerns, unfortunately render access to information and civic participation they may afford inaccessible to those who are unable to pay for their services. On the flip side, in “free” models often employed by technological service providers such as Facebook or Google for a number of its services, a user’s personal data pays for access to these spaces. This practice makes these services accessible to a wider audience, but risks infringement of fundamental consumer privacy principles.

¹ Boyd, Danah. *it’s complicated*. Yale University Press. 2014.; Woelfer, Jill. “Homeless Young People’s Experiences with Information Systems: Life and Work in a Community Technology Center.” *CHI 2010*. 207. 10–15 Apr., 2010. Atlanta, Georgia.; Kahne, Joseph, Nam-Jin Lee and Jessica T. Feezell. “The Civic and Political Significance of Online Participatory Cultures among Youth Transitioning to Adulthood.” *Journal of Information Technology & Politics*, 10:1, 1-20. 2013. <https://doi.org/10.1080/19331681.2012.701109>; Steinfield, Charles, Nicole B. Ellison and Cliff Lampe. “Social capital, self-esteem, and use of online social network sites: A longitudinal analysis.” *Journal of Applied Developmental Psychology*, 29, 434–445. 2008. <https://doi:10.1016/j.appdev.2008.07.002>; boyd, danah. “Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life.” *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume* (ed. David Buckingham). Cambridge, MA: MIT Press. 2007.; Bell, Genevieve and Paul Dourish. “Yesterday’s tomorrows: notes on ubiquitous computing’s dominant vision.” *Personal Ubiquitous Computing*, 11: 133. 2007. <https://doi.org/10.1007/s00779-006-0071-x>.

² “4 news media companies share digital subscription revenue models.” International News Media Association (INMA). Accessed December 14, 2017. <https://www.inma.org/blogs/conference/post.cfm/4-news-media-companies-share-digital-subscription-revenue-models>.

Personal data that users provide referenced above may be in the form of what I will refer to conscious provision (i.e. entering a name, an email address, a social security number, etc. into a provided field), or in many cases unconscious provision (i.e. clicking on an advertisement while using a tech service, thereby providing the tech service provider with personal behavioral information about the user's product or information preferences).

It is unclear whether both of these data types are implied by this document's use of the phrase "personal information they provide to organizations." Indeed, if both these data types are implied, the idea of a consumer having the ability to exercise control over the collection, user, storage, and disclosure of this personal information becomes significantly more complex than if only the former consciously provided data. Since the latter unconsciously provided data is closely tied to technological companies' generation of profit under current business models, it is unclear how, exactly, consumers can exercise control over this data if any given current conceptions of profit generation that rely in part on data collection practices being intransparent. As Steimer writes, "Data collection must have consumers' approval, but to avoid the "ick" factor of seemingly creepy ad targeting, the curtain can't be pulled away completely to reveal all of marketing's tricks."³ Related, Samuel writes, "as long as these companies run on advertising revenue, they have little incentive to promote transparency among data brokers and advertisers. And those industries, in turn, have little motivation to place ethics ahead of profit."⁴ Under current profit models, the notion of consumers having access to and control over their personal data remains of questionable feasibility.

Given this ambiguity in how the document defines "personal information they [consumers] provide to organizations", it is especially important that the document clarify its definition of the term "reasonable," as in its current use it is unclear what "reasonable" might entail and seems to leave significant wiggle room for technological services providers to interpret in such ways that averse to consumer privacy interests.

Related, in reference to the following quotation in section A5 ("Access and Correction") of the document:

"Users should have qualified access [to] personal data that they have provided, and to rectify, complete, amend, or delete this data."

whether or not this ideal is feasible depends largely on whether this document includes unconsciously provided data in its definition of "personal information they provide to organizations" in section A2.

Section A5 further goes on to state:

³ Steimer, Sarah. "The Murky Ethics of Data Gathering in a Post-Cambridge Analytica World." *American Marketing Association*. 31 May 2018. Accessed 3 Oct. 2018.
<https://www.ama.org/publications/MarketingNews/Pages/marketers-are-wading-through-an-online-data-swampland.aspx>.

⁴ Samuel, Alexandra. "The shady data-gathering tactics used by Cambridge Analytica were an open secret to online marketers. I know, because I was one." *The Verge*. 25 Mar. 2018. Accessed 3 Oct. 2018.
<https://www.theverge.com/2018/3/25/17161726/facebook-cambridge-analytica-data-online-marketers>.

“This access and ability to correct should be reasonable, given the context of the data flow, appropriate to the risk of privacy harm, and should not interfere with an organization’s legal obligations, or the ability of consumers and third parties to exercise other rights provided by the Constitution, and U.S. law, and regulation.”

Again, the implied meaning of the word “reasonable” is unclear and appears to leave significant room for interpretation in ways that may allow technological service providers to circumvent the privacy principles intended by this document. Further, the phrase “ability of consumers and third parties to exercise other rights provided by the Constitution, and U.S. law, and regulation” raises a question as to what “other rights” are implicated here. Which rights is this statement referring to? Which rights are implied would seem to be of significant importance to determining how a technological service provider can enforce the document’s privacy principles, third parties’ ability to access and uses consumers’ personal information, and consumers’ understanding of the power they have to exercise their right to privacy as outlined by this document.

In response to Question C2 (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?)

In accordance with those issues discussed in response to question A2, and the described underlying perceived conflict of interests between current private sector profit models and consumer privacy needs, I would urge the Department to consider convening a working group to evaluate how to balance:

1. Technological service providers’ private sector profit-making needs and interests;
2. These companies’ social responsibilities as entities responsible for providing access to information and digital civic spaces;
3. Consumers’ privacy needs and interests;

with and end goal of generating innovative approaches to profit-making business models that meet U.S. civil society’s and individual U.S. consumers privacy needs and interests. These outputs may manifest in the production of:

1. Leading technological service providers commitment to implementing pilot versions of the profit-making models generated by the working group;
2. Regulatory recommendations to the Federal Communications Commission concerning how they might be able to support innovation according to approaches suggested by the working group;
3. Proposed modifications to the National Telecommunications and Information Administration’s approach to consumer privacy.

I would suggest that this working group consider looking to examples of other industries that have managed fairly strict consumer privacy protections while still generating significant profit (i.e. health insurance industry’s profitable success while still achieving consumer privacy protections outlined by HIPAA) and legal codes pertaining to how libraries and other public information sharing institutions protect the privacy of their clients while at the same time

providing civic spaces (i.e. state privacy laws regarding library records <http://www.ala.org/advocacy/privacy/statelaws>)⁵.

Following, I would suggest that those parties invited to participate in such a working group include relevant representatives from each of:

1. Major consumer-data collecting technological service providers;
2. Major libraries, archives, or heritage organizations;
3. Major health service providers;
4. Major consumer privacy advocacy organizations;
5. The Federal Trade Commission (enforcer of consumer privacy regulations);
6. The Federal Communications Commission (enforcer of interstate information exchange and communications regulations).

⁵ “State Privacy Laws Regarding Library Records.” *American Library Association*. 2018. <http://www.ala.org/advocacy/privacy/statelaws>.

Works Cited

- "4 news media companies share digital subscription revenue models." International News Media Association (INMA). Accessed December 14, 2017.
<https://www.inma.org/blogs/conference/post.cfm/4-news-media-companies-share-digital-subscription-revenue-models>.
- Bell, Genevieve and Paul Dourish. "Yesterday's tomorrows: notes on ubiquitous computing's dominant vision." *Personal Ubiquitous Computing*, 11: 133. 2007.
<https://doi.org/10.1007/s00779-006-0071-x>.
- boyd, danah. *it's complicated*. Yale University Press. 2014.
- boyd, danah. "Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life." *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume* (ed. David Buckingham). Cambridge, MA: MIT Press. 2007.
- Kahne, Joseph, Nam-Jin Lee and Jessica T. Feezell. "The Civic and Political Significance of Online Participatory Cultures among Youth Transitioning to Adulthood." *Journal of Information Technology & Politics*, 10:1, 1-20. 2013.
<https://doi.org/10.1080/19331681.2012.701109>
- Samuel, Alexandra. "The shady data-gathering tactics used by Cambridge Analytica were an open secret to online marketers. I know, because I was one." *The Verge*. 25 Mar. 2018. Accessed 3 Oct. 2018. <https://www.theverge.com/2018/3/25/17161726/facebook-cambridge-analytica-data-online-marketers>.
- "State Privacy Laws Regarding Library Records." *American Library Association*. 2018.
<http://www.ala.org/advocacy/privacy/statelaws>.
- Steimer, Sarah. "The Murky Ethics of Data Gathering in a Post-Cambridge Analytica World." *American Marketing Association*. 31 May 2018. Accessed 3 Oct. 2018.
<https://www.ama.org/publications/MarketingNews/Pages/marketers-are-wading-through-an-online-data-swampland.aspx>.
- Steinfeld, Charles, Nicole B. Ellison and Cliff Lampe. "Social capital, self-esteem, and use of online social network sites: A longitudinal analysis." *Journal of Applied Developmental Psychology*, 29, 434–445. 2008. <https://doi:10.1016/j.appdev.2008.07.002>.
- Woelfer, Jill. "Homeless Young People's Experiences with Information Systems: Life and Work in a Community Technology Center." *CHI 2010*. 207. 10–15 Apr., 2010. Atlanta, Georgia.