From: Sebastian Benthall
To: privacyrfc2018
Subject: Docket No. 180821780– 8780–01 - Comment
Date: Friday, October 26, 2018 8:08:52 AM

To whom it may concern,

Thank you for the opportunity to comment on Docket No. 180821780– 8780–01, "Developing the Administration's Approach to Consumer Privacy".

This note contains several comments. They are organized by specific questions in the RfC.

(A)2. Are the descriptions [of core privacy outcomes] clear? Beyond clarity, are there any issues raised by how any of the outcomes are described?

A core privacy outcome is **transparency:**

> "Organizations should be transparent about how they collect, use, share, and store users' personal information."

The outcome of transparency reflects the desire to enable users to make informed decisions about whether and how to interact with organizations that process their personal information. Transparency is the mitigation of opacity; the definition of transparency as an outcome conflates several distinct sources of opacity which have been studied especially in the case of algorithmic systems. Burrell (2016) identifies three distinct kinds of opacity: (1) opacity resulting from intentional corporate secrecy, as in the case of trade secrecy and intellectual property, (2) opacity due to the technical illiteracy of users, and (3) opacity due to the characteristics of complex machine learning algorithms and the scale at which they operate. The definition of 'transparency' as an outcome would be strengthened if it were more specifically the remedy to one of these three forms of opacity, or else split into several different outcomes. Each form of opacity has different practical remedies.

The RFC mentions the problems with "lengthy notices", which do not achieve the outcome of transparency adequately. The failure of these notices to achieve this outcome may be attributed to any of these three kinds of opacity. Notices may intentionally obfuscate corporate practices; they may be too complicated for normal users to understand; they may simply be unable to communicate the technical complexity used by organizations in practice.

A core privacy outcome is **security:**

> "Organizations should employ security safeguards to protect the data that they collect, store, use, or share."

The *security* measures indicated by the definition of this outcome refer to protection of data from unauthorized use. This envisions security as a problem "from below", as unauthorized actors may breach cyberphysical systems that contain personal information. Due to the complex supply chains that personal data processing systems depend on, and the fact that a vulnerability may be inserted, maliciously or

unintentionally, in a system via any component in the supply chain (Woods and Bochman, 2018; Benthall et al., 2016), cybersecurity due diligence is not easily handled within the bounds of a single organization. As the recent passing of FIRRMA expanding CFIUS's powers indicates, a key cybersecurity risk for many organizations is that some part of their supply chain is coopted "from above" through shareholder buyout or state intervention. These interventions may be "authorized" from a computer security perspective, but may nevertheless open personal information to adversarial exposure. A clearer distinction between these kinds of security problems could shine light on the path toward achieving security as an outcome.

(C)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?

The outcome of *transparency* is in part to mitigate the problems of opacity in algorithmic systems. A key source of opacity, identified by Burrell (2016), is intentional corporate secrecy about business processes. A solution to this form of opacity is an enriched ecosystem of open standards and open source software implementations of those standards. This ecosystem can be enriched directly through investment via government procurement preferential to open software and open standards. A limited form of this policy can be found in the existing Federal Source Code Policy (https://sourcecode.cio.gov/); the provisions about procuring open source software can and should be strengthen to support algorithmic accountability in the use of personal information.

(C)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?

Commercial data privacy and finance have in common that there is often a large disparity between the information available to the consumer of a service and the information available to a supplier. In many cases in finance, this is solved by legally guaranteeing that the service provider has a fiduciary relationship with the customer. Balkin (2015, 2018) has proposed that governments should treat data processors as fiduciaries, with duties of good faith and non-manipulation towards their clients. The Department can convene people and organizations to explore the possible legal bases for such a stance.

A related course of action would be to connect the Adminstration's approach to consumer privacy to the Administration's approach to Software Component

Transparency, a topic about which NTIA is already convening multistakeholder meetings. While consumer protection of personal data, software system security, and software system accountability have often been addressed in separate intellectual and industrial silos, these distinctions are artificial and their respective communities have much to learn from each other.

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?

Given that the harms due to personal information disclosure and use can have broad social effects external to transactions between organizations and individual users, the FTC's mandate to prevent unfair and deceptive practices is inadequate to empower it address these adequate privacy harms.

Data flows are better understood as changing elements to an economic strategic field than individual market transactions (Benthall, 2018), and hence regulatory powers fitted to areas of commerce focused on the staking out of market positions under conditions of uncertainty may be more appropriate. Financial regulation institutions such as the Security Exchange Commission, in particular, may be the appropriate model for an empowered privacy enforcement agency. Further research is needed to determine the strength of the parallels between privacy risk and risks to the financial economy, and the concrete policy implications of those parallels.

Best regards,

Dr. Sebastian Benthall
Research Scholar
Center for Cybersecurity
NYU

References

Balkin, Jack M. "Information Fiduciaries and the First Amendment." *UCDL Rev.* 49 (2015): 1183.

Balkin, Jack M. "Free Speech is a Triangle." (2018).

Benthall, Sebastian. "Context, Causality, and Information Flow: Implications for Privacy Engineering, Security, and Data Economics." (2018).

Benthall, S., Pinney, T., Herz, J., Plummer, K. (2016) An Ecological Approach to

Software Supply Chain Risk Management. *Proceedings of the 15th Python in Science Conference*. p. 136-142. Ed. Sebastian Benthall and Scott Rostrup.

Burrell, Jenna. "How the machine ‘thinks’: Understanding opacity in machine learning algorithms." Big Data & Society3.1 (2016): 2053951715622512. http://journals.sagepub.com/doi/pdf/10.1177/2053951715622512

Strandburg, Katherine J. "Free fall: The online market's consumer preference disconnect." U. Chi. Legal F. (2013): 95. https://lsr.nellco.org/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1433&context=nyu_plltwp

Beau Woods and Andy Bochman, “Supply chain in the software era”. Whitepaper. Atlantic Council, 2018. http://www.atlanticcouncil.org/publications/issue-briefs/supply-chain-in-the-software-era