PRIVITAR
open data | protect privacy

Privitar Response to US Department of Commerce National Telecommunications and Information Administration Request for Comments

November 2018

Consultation on Developing the National Telecommunications and Information Administration's Approach to Consumer Privacy

This response is from Privitar. Privitar is a global enterprise software company, headquartered in London. Privitar's US offices are in San Francisco and New York City.

Privitar's mission is to promote and facilitate the ethical and safe use of valuable data assets. Using the most advanced privacy engineering techniques, we help companies get maximum value from data while preserving customer's privacy.

Privitar welcomes the National Telecommunications and Information Administration's (NTIA) Request for Comment (RfC). Privitar supports this initiative and believes the United States of America (US) would benefit from more robust privacy standards. Privitar agrees with many of the positions taken, especially the recognition that technology has an important role to play in mitigating and managing privacy risk. Privitar is keen to engage with the NTIA as they develop their position and hopes that the comments below can be the start of a discussion about how best to improve privacy standards to boost trust and enable responsible innovation in the US.

Response to RfC questions

1. Response to A3. *"Are there any risks that accompany the list of outcomes, or the general approach taken in the list of outcomes?"*

i. There is the need for an alternative legal basis to consent

Privitar agrees with points made by the NTIA on the weaknesses of consent only models. Specifically, Privitar believes consent should be seen in the light of:

a. Consent is not a goal in and of itself. Consent is a tool for protecting fundamental rights and freedoms, where it is not effective at doing so then it should not be used.
b. 'Consent fatigue' and limits on 'mental bandwidth' make consent a tick box exercise. Users are not able to meaningfully engage with many of the choices they're asked to make.
c. The increasingly complexity of data architectures and processing purposes means that many users lack a meaningful understanding of the risks and benefits involved in consenting to their data being processed.
d. The powerful effects of choice architecture. By controlling how users interact with products, data controllers can manipulate user choices and cause them to act against their better interests.

e. The limited alternatives. Consent is not a meaningful protection when there isn't a realistic alternative, or range of alternatives.

The result of these factors is that users are often placed at a disadvantage and consent alone does not protect them. Instead, many countries have looked to alternative approaches for protecting fundamental rights and freedoms in some situations, such as the 'legitimate interest' basis for processing in the EU. Last year Singapore's data protection authority, the PDPC, held a public consultation on 'Approaches to Managing Personal Data in the Digital Economy'. One of the objectives of the consultation was to gather views on whether the PDPC should expand the legal bases for data processing to include 'legitimate interest'. The conclusion[1] of the consultation was to expand the legal bases. Privitar's comments on the proposal can be read here[2]. It may be worthwhile for the NTIA to engage with the PDPC to better understand their reasoning and what they learn from the consultation.

When considering legitimate interest as a legal basis for processing, it is worth considering:

a. The purpose of using legitimate interest is either to enable processing where it is not appropriate to engage with the user, or where consent does not effectively protect the user. In the case of the latter, legitimate interest should not take away an individual's ability to make decisions about how their data is processed. It is there to raise the default protections, not to prevent individuals from exerting autonomy about how their data is used. As such the legitimate interest basis should be complemented by a strong and easily accessible right to object to processing. Such that data subjects who do not wish for their data to be processed on the basis of a legitimate interest, can easily exercise this right where it is reasonable to do so.

b. Using the legitimate interest basis under the GDPR places the responsibility on the data controller to make sure that their processing does not put the user at risk. To be effective, this means that controllers need to both have appropriate policies and controls and apply them effectively. This is generally self-regulated, with regulators usually only becoming involved if something has noticeably gone wrong. The GDPR deals with the need for more regular oversight by creating the role of the Data Protection Officer (DPO). The DPO acts as an internal regulator. This may be effective

[1] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/PDPC-Response-to-Feedback-for-Public-Consultation-on-Approaches-to-Managing-Personal-Data-in-the-Dig.pdf

[2] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Responses-Received-as-at-5-October-2017/privitar.pdf

and may not. DPOs have been required in Germany since 2001, and so more evidence can likely be found by looking at the German experience. Alternatively, other mechanisms may be necessary, such as allowing consumer rights groups rights of access and audit, or requiring the publication of specific policies and internal audit reports.

ii. Solely outcome-based approaches may not be sufficient

Whilst Privitar welcomes a risk-based approach to privacy in general, a solely outcome-based approach is potentially vulnerable to certain kinds of privacy harms. Many privacy harms are hard to detect and delayed in impact. As such a model which is solely ex post may permit certain harms occurring systemically, and lack effective mechanisms for preventing them becoming widespread.

For instance, a growing unease and belief in ubiquitous monitoring may lead to a general erosion of trust in public entities and growing social disengagement. This can be a powerful social harm but may be very difficult to attribute to a specific practice or individual action. As such, where harms are delayed and difficult to measure, ex ante protections may be needed. Privitar would suggest that the NTIA assess which privacy harms would, and which would not, be detectable under their outcomes-based model and then consider whether some more prescriptive protections may be needed in some instances. Privitar believes that a robust data protection framework likely requires both ex ante and ex post protections.

iii. Looking beyond minimisation

Privitar welcome's the NTIA's proposals around data minimisation. We believe that this agenda could usefully be extended by looking at other strategies for reducing the risk associated with processing data. To this end we would suggest reviewing Jaap Hopeman's work[3] on privacy by design strategies. These include 'minimisation', but also include other data-based strategies, such as 'hide', 'separate' and 'aggregate'.

2. Response to C1. *"Are there any aspects of this approach that could be implemented or enhanced through Executive action, for example, through procurement? Are there*

[3] https://www.cs.ru.nl/~jhh/publications/pdp.pdf

any non-regulatory actions that could be undertaken? If so, what actions should the Executive branch take?"

Many organisations could significantly reduce the privacy risks created by their data processing by using privacy enhancing technologies which are available today. The field of privacy engineering and privacy enhancing technologies (PETs) is full of well-developed tools and techniques. However, awareness of these tools is low and publicly available case studies of how they have been implemented are rare. ENISA's work on PETs readiness[4] provides 6 tiers of technological maturity. Many PETs have been proven in principle many times but lack a wide base of use cases to enable their broad adoption.

The US Government could support the adoption of PETs by acting as an early buyer and publishing reports on their projects and use of PETs so that other organisations can learn from the US Government's experience. Setting high federal standards for use of PETs would both help industry and reduce privacy risk in the Federal Government.

3. Response to 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?"*

Privitar believes that technology has an important role to play in protecting individuals' rights and freedoms and enabling organisations to use their data freely and innovatively. As described above, a major hurdle to the use of technologies which facilitate this is a lack of awareness and understanding of what technologies are available. As such Privitar would recommend that the NTIA use this opportunity to bring together those working on PETs with organisations, from the public and private sector, facing privacy challenges, so as to identify where PETs can be applied to enable data use and reduce privacy risk.

In the UK the Royal Society is currently carrying out a review of PETs which will aim to provide policy advice to HM Government and industry on the state of five key technologies and how they could be used. It may be worth the NTIA engaging with the Royal Society to share learning and review the Royal Society report once it has been published.

[4] https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-pets-maturity-assessment-methodology

4. Response to C3. *"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?*

Privitar questions whether the current patchwork of privacy regulations in the US is the most effective way of ensuring consistent and robust privacy protections in the US. Whilst we accept that a regulatory overhaul may not be feasible in the current political setting, we believe that in theory it might be the most desirable path.

In the absence of that possibility, we believe that it would be helpful to review Section 5 of the FTC and re-evaluate whether the FTC is currently both tasked and empowered to sufficiently protect consumer privacy in the US.

5. Response to 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…*

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

4. What should those definitions be?"

i. Moving away from use of the term 'PII'

We noted that the RfC uses the terms 'personal information' and 'personal data' rather than PII. We support this and would encourage the Department and others to move away from using the terms PII and non-PII on the basis that, as perhaps the NTIA is aware, PII can be a misleading term. 'PII' implies that there exists a category 'non-PII' which simultaneously relates to an individual but is not identifying. However, increasingly this distinction is not meaningful; information that had been classified as non-PII but relates to individuals can often be associated with those individuals and is vulnerable to re-identification through linkage attacks.

ii. Distinguishing between different categories of data

We would also encourage the distinction between different categories of data based on the risk that their use and dissemination is likely to present to data subjects. Specifically, distinguishing between:

a. Directly identifying micro data. By micro data, or row level data, we mean data where the data points relate to single individuals, as opposed to aggregate data, where the data points relate to groups of individuals. By directly identifying we mean that the data contains direct identifiers such as name or account number. Values which are likely to allow others to identify who the data relates to without significant effort being required. Whilst privacy risk depends on many factors, such as the environment the data is being processed in, and the sensitivity of the data, generally speaking row level data is the highest risk data type. As such its use should be restricted, and organisations should be encouraged to only use it when it is demonstrably necessary.

b. Pseudonymous micro data. Also known as tokenised or masked data. This is data where the direct identifiers have been removed or replaced with alternative values. This prevents users of the data from being able to easily identify whom the data is about. However, pseudonymous data is still vulnerable to linkage attacks, where other data sources are used to re-identify individuals in the data, as such it should still be considered to be personal data.

c. Aggregate data. Often aggregates are mistakenly believed not to leak information about specific individuals. However, this is incorrect, and numerous attacks exist, such as differencing and reconstruction attacks, which allow attackers to learn information about individuals from aggregate data, or, in some instances, even reconstruct the entire dataset used to create the aggregates. As such aggregates about people should also as a default be assumed to be personal data, although they often present a significantly lower risk to individuals than microdata.

d. 'anonymous' data. Additional protections, such as generalisation or perturbation for row level data, or differentially private noise addition or statistical disclosure control methods for aggregates, can defend against the attacks mentioned above and reduce the risk of re-identification such that it is negligible. This is sometimes called anonymisation, but this term can lead to confusion as the term anonymisation is essentially describing a risk threshold, whereas the term is sometimes taken to mean an absolute guarantee of protection of some kind. Setting where this risk threshold should be and how it should be assessed is a difficult challenge, but one which many organisations have been working on, such as the UK's ICO[5] and UK Anonymisation Network[6]. We believe that data which has been appropriately protected in these ways should not be within the remit of privacy laws, as whilst there may continue to be a theoretical risk posed to the data subjects, it is sufficiently low that it should not prevent the use and dissemination of data of this kind.

[5] https://ico.org.uk/media/1061/anonymisation-code.pdf

[6] http://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf

We would recommend that organisations are encouraged to use the lowest risk data possible, ideally this encouragement should be reflected in the behaviour of the FTC with regards to enforcement actions, and the consideration of whether organisations have taken reasonable steps to protect users' privacy when considering liability in the event something goes wrong.

Privitar is keen to engage with NTIA further and would welcome the opportunity to discuss the points made in this response, and others, at the NTIAs convenience.