Comments on the
"Guidelines on transparency under Regulation 2016/679"

December 21, 2017

Background

I am a privacy and trust engineer/consultant with a small boutique consultancy, Enterprivacy Consulting Group located in the United States. I am also a licensed attorney in the the US (State of Florida, Bar #90009). The primary focus of my consultancy is assisting companies in education and development of their "Privacy by Design" programs or, for Article 25 of the General Data Protection Regulation, "Data Protection by Design."

I have been working in Information Security / Privacy for 13 years, hold a CIPP/US, CIPT, CIPM and have been designated a Fellow of Information Privacy by the IAPP. Further, I was designated a Privacy by Design Ambassador by the Information and Privacy Commissioner of Ontario, Canada when that office was issuing such designations. I am a frequent speaker, writer, blogger and tweeter on the subject of privacy. More can be found on my CV at https://enterprivacy.com/about/ and https://twitter.com/privacymaverick

Earlier this year, Professor Daniel Solove, of George Washington University Law School, and I won a competition by the Office of National Coordinator of Health Information Technology for the US Department of Health and Human Safety to create a privacy notice generator for health technology Apps.[1] The essence of that software was to provide an easy interface to allow health technology generator to develop a simple privacy notice to accompany their mobile Apps. While the software was not initially designed meet GDPR requirements, the generated notices easily conformed to the criteria in Article 12 of the GDPR: concise, intelligible, easily accessible and using clear and plain language. Seeing the natural connection, I set out to modify the generator to produce GDPR "compliant" privacy notices and currently provide the tool for purchase on my website: https://enterprivacy.com/gdpr-privacy-notice-policy-template/ [2]

The tool is not meant to substitute for legal advice, but supplement such advice. As such the final resulting notice is provided in HTML and is fully customizable to meet the needs of the organization. Where the tool excels is mostly around accessibility. The design is responsive, so it adjusts for varying screen sizes of devices. The design provides easily read fonts and contrasting colors which meet web accessibility guidelines. The design uses content areas to provide information for non-graphical screen readers, in line with best practices. For those that wish to rely on the text provided, it has been optimized for readability, including simple words, short sentences and active voice. Where a law firm can provide verbal content to comply with a specific organizations practice, the tool provides a wrapper to increase accessibility and standardization. Several enhancements are already planned, including multi-lingual support and implementation of standardized icons, once released.

After having read the Article 29 Data Protection Working Party draft Guidelines, there are two areas that I feel would benefit from additional explanation. They are discussed below.

Ambivalent language

1 See https://iapp.org/news/a/cronk-solove-win-onc-privacy-notice-generator-contest/

2 Compliant is in quotations marks because while compliance is determined by the relation between the information provided and the practices of the data controller, the tool prompts the data controller to complete the necessary elements specified in Articles 13 and 14 and attempts to generate a draft notice that meets the requirements of Article 12.

Paragraphs 11 and 12 of the Guidelines, propose that language in privacy notices should not be abstract or ambivalent, that use of qualifiers like "may" should be avoided. While its understandable that use of ambiguous terms like "marketing purposes" provide limited insight for the data subject into the processing, ambiguity around whether a data subject's information will be used for a particular purpose is necessary in some circumstances.

Consider a grocery store promotion. Every 1000th customer gets 30% off their bill, excluding alcohol purchases. In calculating the 30% discount, the store is processing personal data (the amount of the individual's bill and whether it contains alcohol purchases). Would it be appropriate, or not, to provide notice to shoppers about the promotion which included:

"As part of this promotion, shoppers' bill may be processed to calculate the applicable promotional discount."

Replacing the qualifier "may" with "will" suggests that all shopper's personal data will be process for this purpose, when, in fact, it's only a limited subset (1 out of every 1000). Does changing the language to "…, one of out of a thousand shoppers' bill will be processed..." provide any more clarity? An individual shopper still doesn't know if their data will be used or not. Arguably the precision provide the shopper with an assessment of likelihood (a component of risk), but the additional precision runs counter to the concise requirement and will contribute to information fatigue, especially if done over multiple purposes and instances where processing could take place depending on circumstances.

Further guidance on when qualifiers, like "may," may be appropriate, would be helpful.

Risks

Paragraph 9 of the draft Guidelines cites the needs of data controller to highlight the "*consequences*" of processing. Paragraph 25 quotes Recital 39 on making data subjects "aware of the risks..." in relation to processing data. Paragraph 30 further suggest that layered notices clearly indicate the "consequences of processing." Finally, paragraph 35 acknowledges the recital's stipulation as to "risk, rules, and safeguards" are not explicitly covered in Article 13 and 14.

Risk analysis is part of my data protection by design and default work. Often times it sufficient to eyeball risks, knowing that certain types of data and processing activities increased the risk from privacy violations. Sometimes it is important to actually do more detailed risks analysis.

At the recent US Federal Trade Commission workshop on Informational Harms[3] panelist discussed the consequences of privacy violations. This went much more into detail that the typical discussion of data breaches, talking about a mother losing custody of her children, medical identity theft resulting in misdiagnoses, lost opportunities in housing as a result of processing information about protected classes. I typically use visceral examples in my training, such as the sucides that resulted from the Ashley Madison breach[4] or the murder of Rebecca Schaeffer[5] which spurred the

3 See https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop
4 See http://www.bbc.com/news/technology-34044506
5 See https://en.wikipedia.org/wiki/Rebecca_Schaeffer

US to pass the Drivers Privacy Protection Act. The graphic above at right is based on some of the terminology suggested by the Future of Privacy Forum's "Unfairness by Algorithm: Distilling the Harms of Automated Decision Making"[6] and categorizes many of the consequences of privacy invasions.

As the Working Party is probably aware, few privacy notices delve into the risks and consequences to individuals. Notices typically specify what a company is doing with data, not how it might affect the individual. One can contrast this to the pharmaceutical industry which typically provides side effects warning which excruciatingly detail the negative consequences. An argument can be made that consumers have become desensitized to such warnings as nearly all pharmaceuticals carry a risk of death. The inclusion of such in pharmaceutical warnings is usually the result of a combination of regulatory requirement and a desire to reduce civil litigation, at least in the US.

Sub-paragraphs (f) of Article 13(2) and (g) of 14(2) of the GDPR require privacy notices to detail the "envisaged consequences" of automated decision making but as noted in paragraph 35 of the Guidelines, Recital 39 extends to additional disclosure. My request of the Working Party is to provide further guidance on

- whether Recital 39 requires inclusion of consequences of processing beyond that for automated decision-making in Article 13 and 14
- what form and substance risk and consequences should be relayed to data subjects
- to what extent must consequences be unexpected to be included in a notice[7]

Given that inclusion of risks and consequences are not standard practice in privacy notices to date, I think it's imperative that the Working Party provide more detailed guidance on this topic as well as more forceful instructions to help organizations that may be not reading the Guidelines with careful attention to detail as to recognize the impact this recital may have on privacy notification.

Sincerely,

R. Jason Cronk

I/we hereby consent to the publication of personal data contained in this/the attached document.

6 See https://fpf.org/2017/12/11/unfairness-by-algorithm-distilling-the-harms-of-automated-decision-making/

7 For a service devoted to adulterers, is the risk of a data breach and the consequences of divorce and suicide an expected consequence to which adulterers should be well aware or should they be notified?