European Parliament Hearing on the ePrivacy Regulation

Committee on Civil Liberties, Justice and Home Affairs

11 April 2016

Speech by Benjamin Strahs, Software Engineer at Facebook

Dear Chairman, Dear Rapporteur, Dear Members of the European Parliament,

Thank you for inviting us today. My name is Benjamin Strahs, and I am a software engineer at Facebook, where I'm part of a cross-functional team that supports Facebook Ireland's (the data controller of EU user data) efforts to protect the privacy and safety of the people who use the service.

I am grateful for the opportunity to share Facebook's views on how the proposed Regulation could affect services European consumers rely on and enjoy.

Since the enactment of the ePrivacy Directive, we have seen fundamental changes in the nature of electronic communication services. In the early days of the ePrivacy Directive, people used electronic communication services primarily to send messages from point A to point B. Today people often expect more. They use email services expecting spam filtering, inbox organization, and even translation tools; and they use messaging services like Facebook Messenger expecting that the service will use content to help them do things like set up appointments, get directions, or call a taxi.

Messaging is now an area of intense innovation and development, and I wanted to talk to you today about the services we and others are working on to help people express themselves and stay connected with their loved ones in a safe and secure way.

(1) One example is M Suggestions, which is an assistant inside Messenger that automatically processes messages to prompt you to create events, make plans with friends, order food, and more. It's something we built using artificial intelligence.

(2) We're also using artificial intelligence to improve communication for ALL members of our community. For example, we developed a product called Automatic Alternative Text, which describes the content of pictures to people with impairment. I want to show you how it works for Facebook News Feed: https://www.facebook.com/accessibility/videos/1082033931840331/. The product was developed through the analysis of de-identified descriptions of photos people send through Facebook. We want to make this available in Messenger in the future, and it will, of course, require processing of the content of photos when it is deployed there.

(3) Finally, I want to tell you about our work — and the work of others in the industry — to make people's online

experience safer. Along with other email and messaging services, we process communications data to help find malware and other things that could harm people.

For example, child exploitation content is shared with saddening frequency online, but we and others have developed tools to identify these types of images. We use PhotoDNA (a tool that was developed by Microsoft and academic researchers) to help detect illicit images, so that we can keep our community safe. This is how communication has evolved today. It's smarter, more expressive, and safer. As an engineer, I am excited about the next generation of products that will make the world a more open and connected place. Developments in artificial Intelligence and big data bring a promise of exciting new technologies and experiences.

But the proposed Regulation, as currently drafted, threatens to hold back the artificial intelligence and big data innovation I just described. The Regulation treats these types of technologies as unlawful unless both parties to the communication consent to their use.

At Facebook, we believe strongly in giving people control over what happens to their data. In some cases, this happens through consent. But an overreliance on consent will diminish its value in delivering transparency and control. Here's why:

- **Prompting for consent too frequently undermines control**. Research has shown that when people see pop-up screen after pop-up screen, they are trained to click through and progressively give less thought to each click. When we ask for consent at unnecessary times, we make consent less meaningful in those moments when it's necessary. People will tune out.

- **Bad actors won't consent**. Think about the spam, malware, and child exploitation cases I mentioned above. If you were a bad actor, why would you agree to such processing? I fear requiring such tools to be opt-in effectively gives the bad actor an *opt-out*.

- **Consent requirements can slow the development of new services**. The core component of so-called 'big data' is the processing of previously collected data for other purposes — including, perhaps most importantly, the development of new data-driven services. Having to secure consent (as opposed to other legal basis for processing personal data) before using previously collected data for each new purpose can dramatically slow (or even stop altogether) the development of these services — including services like Automatic Alternative Text.

For all these reasons, we are concerned that the proposed Regulation's emphasis on consent for processing communications data will deter development of services like Facebook Messenger. We believe the Parliament has an opportunity to reform the proposal so that it does more to encourage growth in these services while also protecting privacy. In closing, I would again like to thank the Committee for inviting me to speak today. And I look forward to the conversation about the proposed Regulation.