

ICDPPC Global Privacy and Data Protection Awards

2018

Entry Form

Deadline 29 June 2018

To submit an entry to the ICDPPC Global Privacy and Data Protection Awards please complete and email this form to ExCoSecretariat@icdppc.org no later than 29 June 2018.

Note: ICDPPC member authorities can submit as many entries as they wish but a separate form should be used for each different entry. Please complete the entry in English.

1. Contact details for this entry:

- a. Name and email address of person completing this form:
- b. Name of Data Protection or Privacy Authority:

2. Eligibility: By submitting this entry I confirm that:

- a. The Authority is a member of the International Conference of Data Protection and Privacy Commissioners.
- b. The initiative described in this entry was undertaken since the last edition.
- c. I am aware that the information in the entry (other than the contact details in 1(a) above) will be publicised by the ICDPPC Secretariat.

3. Please indicate which **category or categories you wish to enter (delete those that do not apply; you can enter multiple categories):**

- ~~a. Education and public awareness~~
- b. Accountability
- ~~c. Dispute resolution and enforcement~~
- d. Innovation
- ~~e. People's Choice~~

4. Description of the initiative

- a. Please provide a brief summary of the initiative (no more than 75 words):

FTC Recommends Steps to Improve Mobile Device Security Update Practices -

A new FTC report finds that the complexity of the mobile ecosystem means that the security update process for patching operating system software on some mobile devices is intricate and time-consuming. The report recommends that manufacturers consider taking additional steps to get more security updates to user devices faster. It also recommends that manufacturers consider telling users how long a device will receive security updates and when update support is ending.

- b. Please provide a full description of the initiative (no more than 350 words):

A new FTC report finds that the complexity of the mobile ecosystem means that the security update process for patching operating system software on some mobile devices is intricate and time-consuming. The report recommends that manufacturers consider taking additional steps to get more security updates to user devices faster. It also recommends that manufacturers consider telling users how long a device will receive security updates and when update support is ending.

The FTC report offers several recommendations on ways to improve the security update process:

- Government, industry and advocacy groups should work together to educate consumers

about their role in the update process and the significance of updates.

- Industry should build security into support culture and further embed security support considerations into product design, consistent with the costs and benefits of doing so. To that end, industry should ensure that devices receive security updates for a period of time consistent with consumers' expectations.
- Manufacturers should consider keeping better records about update decisions, support length, update frequency, and update acceptance so that they can learn from their past practices.
- Companies should continue streamlining the security update process. In particular, manufacturers should consider issuing security-only updates instead of bundling security patches with general software updates.
- Manufacturers should consider adopting and disclosing minimum guaranteed support periods for their devices and notifying consumers when support is about to end.

- c. Please explain why you think the initiative deserves to be recognised by an award (no more than 200 words)

Consumers use their mobile devices for a wide range of activities and want to have confidence that when they use them they will be secure. The report found, however, significant differences in how the industry deploys security updates and that more needs to be done to make it easier for consumers to ensure their devices are secure.

Security researchers and government agencies agree that it is important to install security updates that patch vulnerabilities in the device's operating system. Many of these devices, however, remain without important security updates for long periods— either because no update is issued at all, because approving and deploying a patch is a lengthy process, or because users do not install available updates. The FTC report examines certain manufacturers' security update practices and offers recommendations on how to improve the security update process.

A key finding of the report is that support periods, the time during which a device receives operating system updates, and update frequency vary widely, even among devices that cost the same, are made by the same company, or are serviced by the same carrier. A device may receive security updates for many years – or, in some instances, may not receive any updates at all.

- d. Include a photograph or image if you wish (note this will help illustrate the description of the entry on the ICDPPC website; the image can be pasted into the entry or send as an attachment or a link may be provided):

- e. Please provide the most relevant link on the authority's website to the initiative (if applicable) (The website content does not need to be in English):

<https://www.ftc.gov/news-events/press-releases/2018/02/ftc-recommends-steps-improve-mobile-device-security-update>

- f. Please provide any other relevant links that you wish that help explain the initiative or its impact or success (e.g. links to news reports or articles):

<https://www.insideprivacy.com/united-states/federal-trade-commission/ftc-issues-report-on-mobile-device-security-updates/>

<https://www.lexology.com/library/detail.aspx?g=04afe3c5-6cca-4d20-b921-36480c3e6760>