What does the GDPR mean for IoT?

GUEST CONTRIBUTOR

Aman Brar

Openwave Mobility Inc.

21 May 2018

Unless you have been hiding in a cave, you have probably heard of the GDPR(General Data Protection Regulation). And it comes into force on May 25th. Its impact will be far-reaching. Companies who are not in the EU — or soon to be out of the EU — are not exempt if they have any dealings with customers in the EU. Much time has been spent preparing for this new regulation and, if the sales emails in our inboxes are anything to go by, businesses are finally buckling down to the task of gaining explicit consent from their customers about the personal data they collect, process and store.

IoT complications

The GDPR will be far-reaching in other respects too: It will extend to IoT devices and their networks. What is far less clear is how organizations will be able to achieve compliance in IoT GDPR. While the advice offered to businesses on more

generic GDPR compliance holds true, applying it in an IoT context can be a real challenge thanks to the very nature of IoT devices and the processing that makes IoT business models viable.

Firstly, IoT devices by their nature do not tend to rely on graphical user interfaces, like a phone or laptop, where alerting a customer is fairly straightforward. Secondly, IoT use cases that rely on data processing and analytics in the cloud will have an exponentially more difficult time ensuring compliance. The interaction between the device and the data is far from simple, involves numerous parties and, under the GDPR, responsibility for the data extends across the whole supply chain.

Wink once for no, twice for yes

So, how exactly can someone give consent with IoT devices? In the absence of the standard screen user interface, this can be tricky and no one size fits all. IoT devices are often — by design — discreet and pervasive so the issue of consent is a challenge.

Take the case of a video-enabled smart doorbell. As visitors to a house will ring the doorbell, the homeowner's phone is alerted so he can check who is at the door via the video link. The video doorbell manufacturer can easily get the homeowner's consent using email communication (or similar) — but how about the consent of any visitors whose image, i.e. data, will be collected, processed — mostly likely in the cloud — and perhaps stored there? Similarly, under the GDPR, consent for personal data can be taken away as well, but it is not clear how this will be applied to many IoT use cases.

Deleting the data trail

Any organization that processes personal information about people must be able to present that data in a unified form should the subject ask to see it. It must do so free of charge, and it must be able to delete that data under the "right to be forgotten" clause. This sounds eminently sensible in protecting individuals' privacy, but when it comes to IoT implementations of any scale, challenges arise.

Take, for example, the networks of CCTV cameras in smart cities. They will need to be able to show a data trail relating to any of the people the cameras capture. It must also be able to excise and delete the data pertaining to any one individual. This is not just hard to do practically speaking, it also has far-reaching implications for maintaining law and order, health and safety, and preventing fraud or other criminal activity.

‘There is a new update available for your IoT device’

We are all used to receiving update notifications when there is a new app or other software release available. However, as individuals, we are not very good at following through with updates, even though they contain features that will make the user experience better and, more importantly, often contain security enhancements.

Guess what? Organizations are not all that much better at updates either in the form of security patching and other fairly basic privacy and security measures. That will need to change under the GDPR. With IoT devices, the job of updating them cannot be left to chance. Privacy and security requirements will need to be “baked in” to the original design process of a device or network or system of storage.

The role of mobile operators

In case of cellular IoT, much of the IoT device data will travel to the cloud via wireless networks, and here mobile operators can help the IoT ecosystem comply with GDPR. Mobile operators can facilitate this by connecting IoT devices to user mobile identity and sharing opaque identifiers with the IoT devices. The opaque identifiers do not identify the actual user; they just provide a link to connect the two together. This can be reset by the end user. The phone screen and keyboard can also be used as devices to review privacy updates and get user consent for connected devices and request data logs.

Perfect timing

The GDPR has taken a lot of legwork, as anybody who has been tasked with the job of ensuring compliance can tell you. It has meant bolting on privacy considerations onto existing processes and systems. It has involved retrofitting "privacy by design." By comparison, with enterprise systems, IoT is the new kid on the block. While the industry has taken off and is growing rapidly, IoT is still in its infancy.

The GDPR presents serious challenges for IoT, but they are not insurmountable. In fact, given how infrequently the EU updates its data regulations (the last time was more than 20 years ago), the GDPR actually could not have come at a better time in the evolution of IoT. It sends a clear message to the IoT community to think carefully and to think hard about privacy features from the get-go. This is a huge opportunity for manufacturers and network operators to work together to build privacy into the fabric of IoT.

All IoT Agenda network contributors are responsible for the content and accuracy of their posts. Opinions are of the writers and do not necessarily convey the thoughts of IoT Agenda.