Apple Submission in Response to NIST Request for Information
Developing a Privacy Framework, Docket No. 181101997-8997-01

January 14, 2018

Apple appreciates this opportunity to comment on NIST's Request For Information (RFI) regarding its proposed Privacy Framework. Apple supports the development of the Privacy Framework and NIST's engagement on this important topic.

At Apple, we believe privacy is a fundamental human right. We have long embraced the principles of privacy-by-design and privacy-by-default, not because the law requires it, but because it is the right thing for our customers. We've proved time and again that great experiences don't have to come at the expense of privacy and security. Instead, they support them.

Every Apple product is designed from the ground up to protect our users' personal information. We've shown that protecting privacy is possible at every level of the technical stack and shown how these protections must evolve over time. Users can protect their devices with Face ID or Touch ID, where their data is converted into a mathematical representation that is encrypted and used only by the Secure Enclave[1] on their device, cannot be accessed by the operating system, and is never stored on Apple servers. In communication, we use end-to-end encryption to protect iMessage and FaceTime conversations so that no one but the participants can access them. On the web, Safari was the first browser to block third-party cookies by default, and we introduced Intelligent Tracking Protection to combat the growth of online tracking.

When we use data to create better experiences for our users, we work hard to do it in a way that doesn't compromise privacy. We ask users for their permission to use their data and we work to minimize the data we collect. One example is our pioneering use of Differential Privacy, where we intentionally add noise to user data and combine it with the data of millions of others so all we see is general patterns, rather than specifics that could be traced back to a user. We think about privacy at all layers of the technical stack, including going as far as to randomize WiFi MAC addresses to reduce the ways an individuals from being tracked as they go about their day. Finally, we provide users with the ability to access, correct, delete, or deactivate their account at privacy.apple.com.

---

[1] The Secure Enclave is a coprocessor fabricated within the system on chip. It uses encrypted memory and includes a hardware random number generator. The Secure Enclave provides all cryptographic operations for Data Protection key management and maintains the integrity of Data Protection even if the kernel has been compromised. See iOS Security Guide, November 2018, https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf.

We believe NIST should consider and incorporate the following four principles into a framework that helps operationalize privacy risk management:

- **Minimization.** Companies should be challenged to minimize the amount of personal data they collect from consumers, including by de-identifying personal data or simply not collecting it in the first place.
- **Knowledge.** As the digital economy becomes increasingly complex, companies need to ensure that consumers are provided with the information they need at the time that they need it — in other words, by focusing not just on transparency, but pertinence. Users should be informed of what data is being collected, and what it is being collected for. Providing timely and relevant notice about the collection of personal information, such as through just-in-time notices, is the only way to empower consumers to make informed decisions about which collections are legitimate, and which are not.
- **Access.** Companies should recognize that data belongs to users, and it should be easy for users to get a copy of, correct, and delete their personal information.
- **Security.** Security is a foundational principle for all other rights. Apple commends NIST the significant work it has done on this principle through the development of the NIST Cybersecurity Framework.

Apple believes that comprehensive federal privacy legislation is the only way to afford all consumers the same, robust privacy protections, and believes these four essential rights should form the baseline for such a law. Even as we make progress towards that important goal, Apple supports the work done by NIST to create a Privacy Framework that reflects and embodies these principles.