BerkeleyLaw
UNIVERSITY OF CALIFORNIA
Berkeley Center for
Law and Business

Berkeley Center for Law and Business
University of California, Berkeley
School of Law
Boalt Hall #7200
Berkeley, CA 94720-7220

Apple's FaceTime Bug Underscores Questions of Privacy Protection

By: Linda M. Blair, J.D. Candidate 2021 | February 11, 2019

An alarming FaceTime video-chat service vulnerability raises questions about Apple's public commitment to security and consumer privacy. A fourteen year old from Arizona discovered the security flaw, which allowed iPhone users to call other users via FaceTime and listen in on conversations, even if the recipient did not answer. In certain instances, the caller was even able to see video of the non-responsive recipient. While Apple regularly boasts about the safety of its products, such security violations go beyond surface level mistakes into the territory of personal privacy, data protection, and even national security.

For many years prior, Apple allowed outside app developers to access, store, share and sell users' contact data, often without consent. In July of 2018, Apple closed that loophole by banning the storage and sale of such data and stepped its data security by offering bounties to hackers that flag bugs to the company. What's more, Apple's reputation as a privacy protector was cemented in the minds of users when the company refused to compromise its stance on iOS security in the face of FBI scrutiny.

But others, including House Democrats and the House Energy and Commerce Committee, are not so easily convinced. While collecting less of our data and de-identifying who it comes from is a good start, leaving consumer data in the hands of independent developers with direct access to iPhone users who are not incentivized to collect and use our data responsibly eats away at those protection headways. Consumer privacy and protection must take serious the need for a system that gives customers more direct control over who has their information.

For a company that has made it a point of heralding as the privacy conscious adult among the other tech giants, Apple might do more to pre-empt security attacks and protect user privacy. Lessons from Facebook's responsibility for the actions of Cambridge Analytica tell us that the company should be more proactive in limiting how developers use iPhone users' data. The proliferation of bugs like the FaceTime glitch could lead to serious privacy breach issues, not to mention the danger of the data landing in the hands of people that commit attacks on our nation. If privacy is indeed the fundamental human right that Apple CEO Tim Cook says it is, more work is needed to ensure that useful tools like our iPhones don't become spying machines for perverse use.