

Going Dark: Are Technology, Privacy and Public Safety on a Collision Course?

Federal Bureau of Investigation Website, October 16, 2014

Speech at Brookings Institution by FBI Director, James B. Comey

<https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>

***Definition:** Going dark means those charged with protecting Americans aren't always able to access the evidence needed to prosecute crime and prevent terrorism even with lawful authority, i.e. possess legal authority to intercept and access communications and information pursuant to court order, but often lack the technical ability to do so.*

Problem statement by Comey is that threats are changing every day, as such FBI would like to possess every lawful tool to keep the public safe from those threats. However, law enforcement struggles to catch up with the pace of technology, so features like Apple's default encryption though a good privacy feature, also protect even the criminals who in this internet age have greater destructive influence capability. Law enforcement is thus, left in the dark given the lawful way to access information of say, Apple customers in through backed up data in the cloud. The probability of cloud data being useful is contingent on criminals and terrorists backing up incriminating data in cloud, which is not likely. Hence, the need for access for law enforcement in order to have a realistic chance at intercepting time sensitive data, which seems like fair price to pay so that law enforcement can keep us safe to enjoy that privacy.

Comey corrects misconceptions stating law enforcement is not asking for a backdoor that would possibly give access to criminals and other enemies of the state, rather, a transparent forward approach abiding by constitutional law. This more so important because time is of great essence to prevent attacks, intercept and prosecute criminals and terrorists. Granted that law enforcement will have access to metadata, it unfortunately does not provide the content of any information. Therefore, unless technology companies comply, law as it related to digital life, is enforced by the terms of the suspected criminals or terrorists.

He resolves by encouraging multi-stakeholder approach to dialogue pertaining to the balance of liberty and security. FBI offers transparency to the public to understand the *what* and *how* of the work done by FBI. In return, the Comey hopes the public will understand that liberty and security can find a common ground, because law enforcement are looking for security that enhances liberty.