
# Session 104-A

# Privacy Versus (In)security: Who Should Win and Why Between Apple and the FBI?


# Session Description

The recent impasse between Apple and the FBI made flash security part of the daily news. The FBI wanted to look at the data in a dead terrorist's cell phone and demanded that Apple unlock the encryption. Apple refused, citing security and privacy issues and noting that governments around the world could demand drive unlocking for almost any reason. Besides, Apple noted, such a backdoor would soon be widely available in an era in which everyone (good and bad) has lots of computing power and plenty of time and ability. So what's the answer? Do we refuse requests from law enforcement that could thwart terrorist attacks and save lives? Do we allow requests and end up with private data being used for blackmailing and spread around the news media? Could we then have lists of police informants, spies, protestors against autocratic governments, or rape victims made public, as well as sensitive corporate data? The specific solution in the Apple/FBI case raises even more questions. The FBI paid a large sum of money (over $1 million) to an unknown vendor to thwart the encryption. Who else could build or buy the same tool?

In the corporate world, both security and recovery are essential. Ideally, we want harmonious co-existence.

This panel will explore the tension between security and data recovery, search for win/win tradeoffs and alternatives, and hopefully elevate the discourse above the irrational, often hysterical, level heard today - we hope! Come join a lively discussion of a fascinating issue.


# Panel Participants

**Organizers:**

Michael Willett, VP Marketing, Drive Trust Alliance
Mike McKean, VP Product Solutions, Fhoosh

**Chairperson/Moderator:**

Michael Willett, VP Marketing, Drive Trust Alliance

**Panelists:**

**Bob Thibadeau**, Chairman/CEO, Drive Trust Alliance

**Derrick Donnelly**, CTO, BlackBag Technologies

**Clifford Neuman**, Director, Center for Computer Systems Security, University of Southern California

**Vijay Ahuja**, President, Cipher Solutions

# Background

- **Strong data security** is essential to private, personal, or business operation and communication
- **Data recovery** is legitimate and proper in selected contexts and under proper protocols
- U.S. Congress is drafting legislation that may not equally recognize the full pro/con;
  possible outcome being draft legislation to **require encryption "back doors"** [1]

  **Draft: "Covered entities that receive a court order for information or data for the investigation or prosecution of specified serious crimes must provide it to the government in an intelligible format or provide the technical assistance necessary to do so."**
- Is there a **win/win** strategy going forward?
- **WHY should flash industry care? IoT is flash memory. Security/Recovery balance will affect acceptance.**
- **History:**

  In the 70s/80s, the U.S. restricted crypto export to 40-bit keys.

  The mistaken belief was that the U.S. was the sole source of good crypto (false).

  U.S. businesses (including IBM) , eventually convinced the govt to lift that restriction.

  Now, we can export strong encryption products, with a one-time review.
- **Points:**

  >>> Security and Recovery: mutually justified requirements, with proper controls

  >>> Legislation needs to be examined methodically for its impact; even practicality.

1: http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649


# Separate Questions

## Apple v FBI

- Should Apple be compelled to comply – No
  - Slippery slope for future orders to compel
  - Compelled speech argument
- Should Apple have complied on their own volition – Yes
  - They had the capability
  - Despite their claims, doing so does not make other devices vulnerable
  - Despite their claims, voluntary acquiescence doesn't create legal precedent.
  - International issues (other governments) already make such requests.
- Why was Apple's assistance requested
  - To sign a specific executable so it could be loaded
- Should we be banning effective encryption/security or requiring backdoors – NO!
  - Misuse of authority – by governments or employees, or in civil matters.
  - Harder to secure or prevent use of backdoors by criminals


# FBI/Apple Kerfuffle Proposed Legislation

Drive Trust Alliance

www.drivetrust.com

Flash Memory SUMMIT

# www.drivetrust.com

Flash SSDs
iPhones, iPads, Android
All of Google etc.
All Printers

Protecting "USER" Data

## A BILLION PEOPLE A DAY USE SELF-ENCRYPTING DRIVE TECHNOLOGY

## There Should Be No Encryption Backdoors, Only Front Doors

"In two sentences: iPhones and iPads have always had front door central encryption management using international standards. The government needs to learn how to legally employ the solutions that companies have employed for over a decade."

READ MORE


# Encryption Central Management

## Encryption Object ID

### Device Owner

Name – Authentication
Create/Delete/Modify Self and Encryption Object, Administrator(s)

### Administrator(s)

Name – Authentication
Create/Delete/Modify Self and More than One User
Create/Delete/Modify Media Encryption Key (MEK)

### Users

Name – Authentication – Key Encryption Keys (KEK)
Create/Delete/Modify Self

## Encryption Object

Data
Verify and Apply User KEKs → Derive and Use MEK


# Characteristics of Proposed Legislation

- Extend HPAA/HITECH Regulation that Requires Encryption Central Management for Data at Rest to areas other than Medical Patient Data.
- **Encryption Law**: Owned assets that contain data that is encrypted must have that encryption under central management. The central management must retain sole custody of at least one valid user credential (KEK). Central management can be provided by any entity that is licensed to provide it.
- **Examples**:
  - All US and Local Government Entities must apply the Encryption Law
  - All Felons must apply the Encryption Law
  - A law generally promotes but does not decree the use of central management for Private Company assets and Family assets