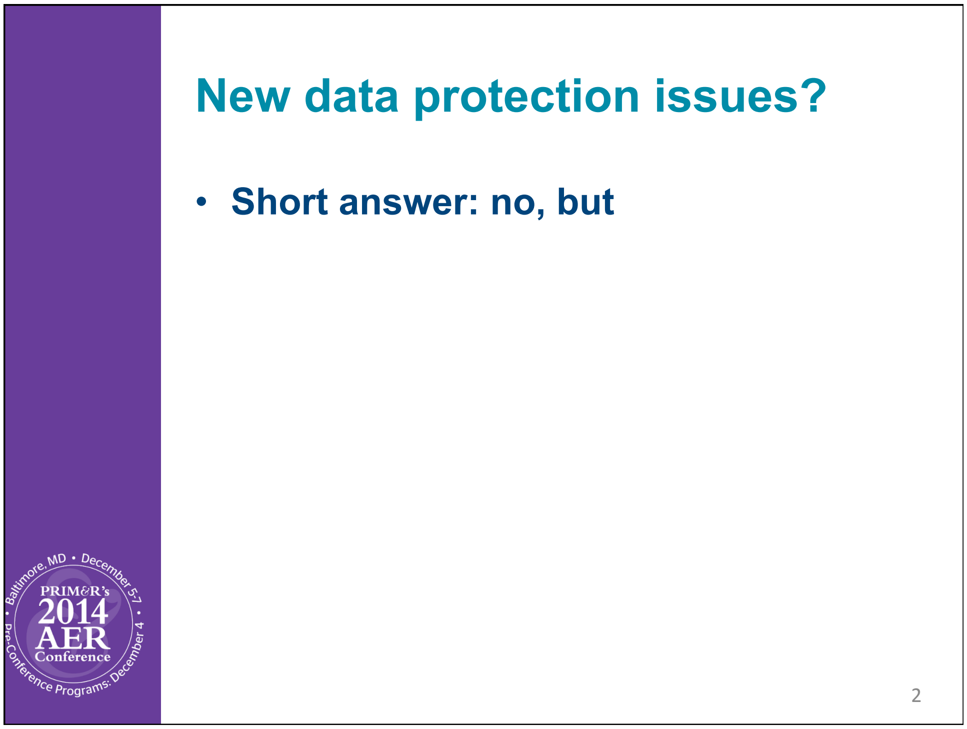
Mobile Devices in Research: Growing tool, new issues?

Scott Bradner

Harvard University

Baltimore, MD • December 5-7 • PRIM&R's 2014 AER Conference • Pre-Conference Programs: December 4

1

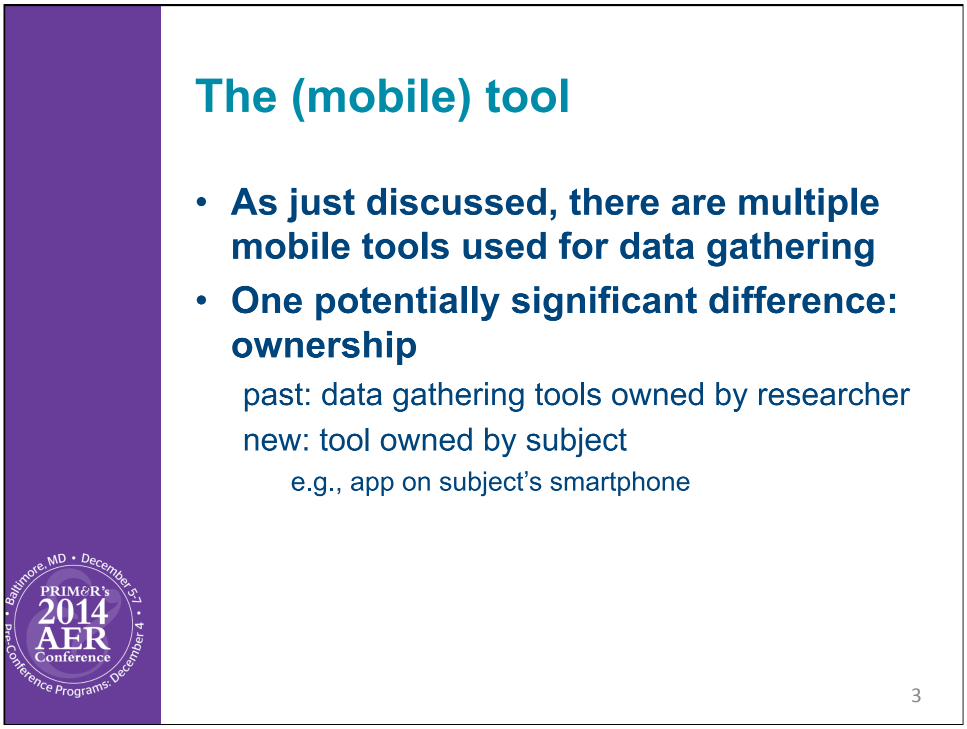


New data protection issues?

- **Short answer: no, but**

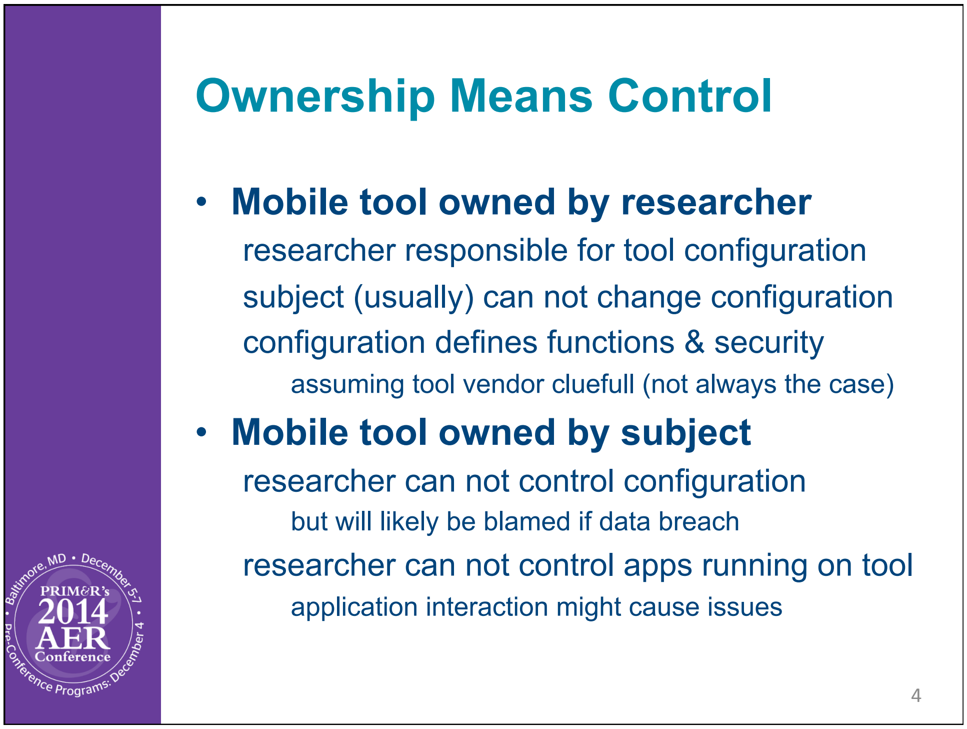
Baltimore, MD • December 5-7 • PRIM&R's 2014 AER Conference • Pre-Conference Programs: December 4

2



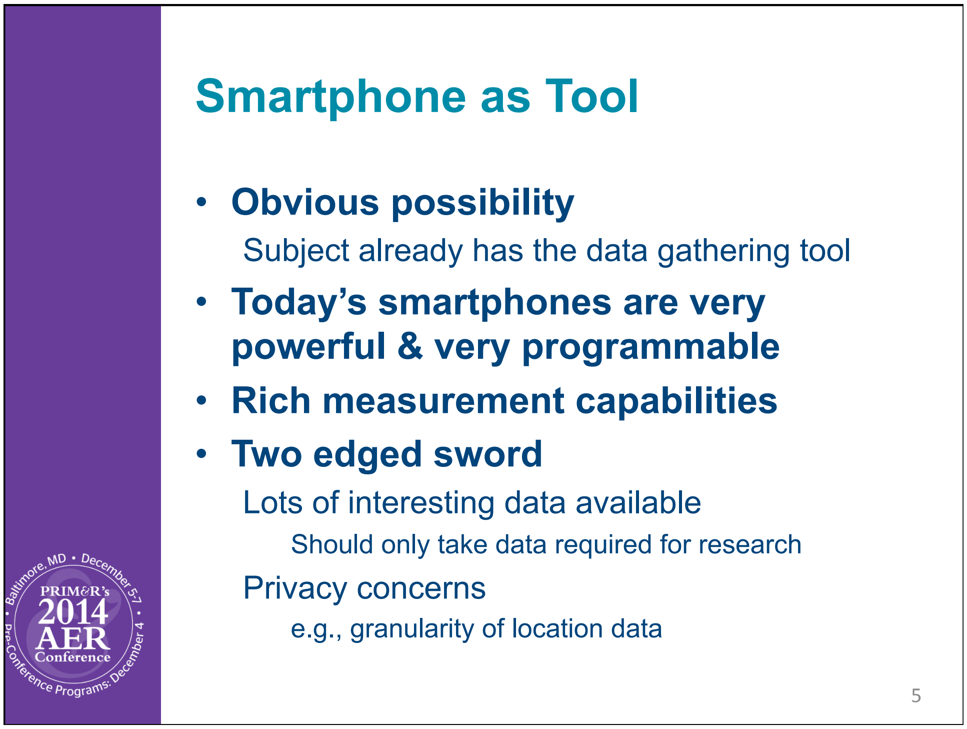
The (mobile) tool

- **As just discussed, there are multiple mobile tools used for data gathering**
- **One potentially significant difference: ownership**
  - past: data gathering tools owned by researcher
  - new: tool owned by subject
    - e.g., app on subject's smartphone



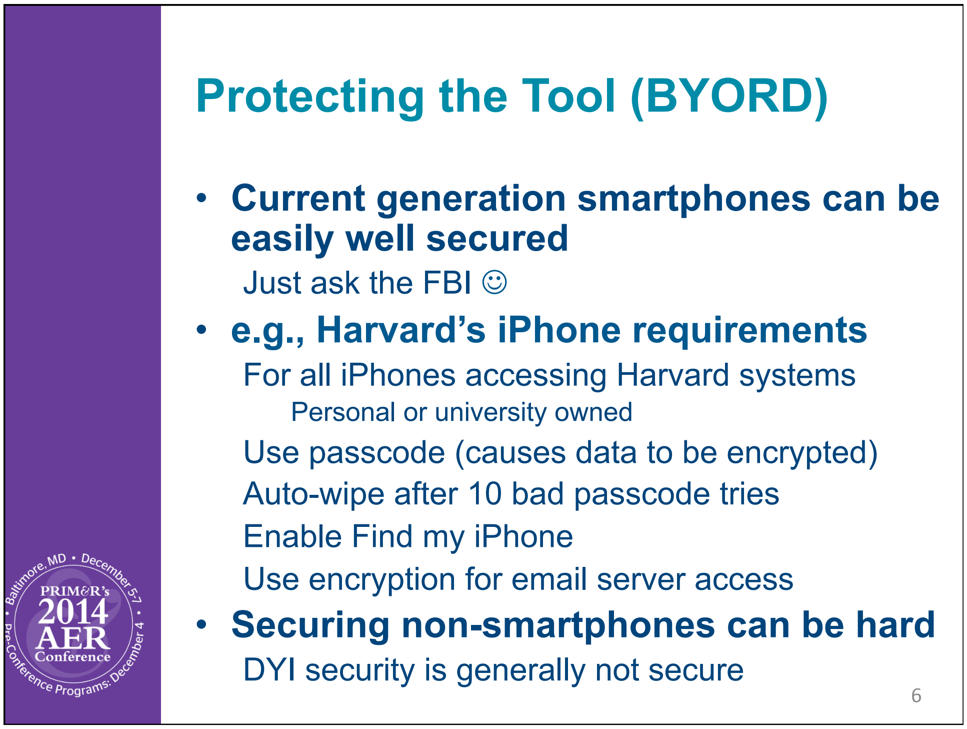
Ownership Means Control

- **Mobile tool owned by researcher**
  - researcher responsible for tool configuration
  - subject (usually) can not change configuration
  - configuration defines functions & security
    - assuming tool vendor cluefull (not always the case)
- **Mobile tool owned by subject**
  - researcher can not control configuration
    - but will likely be blamed if data breach
  - researcher can not control apps running on tool
    - application interaction might cause issues



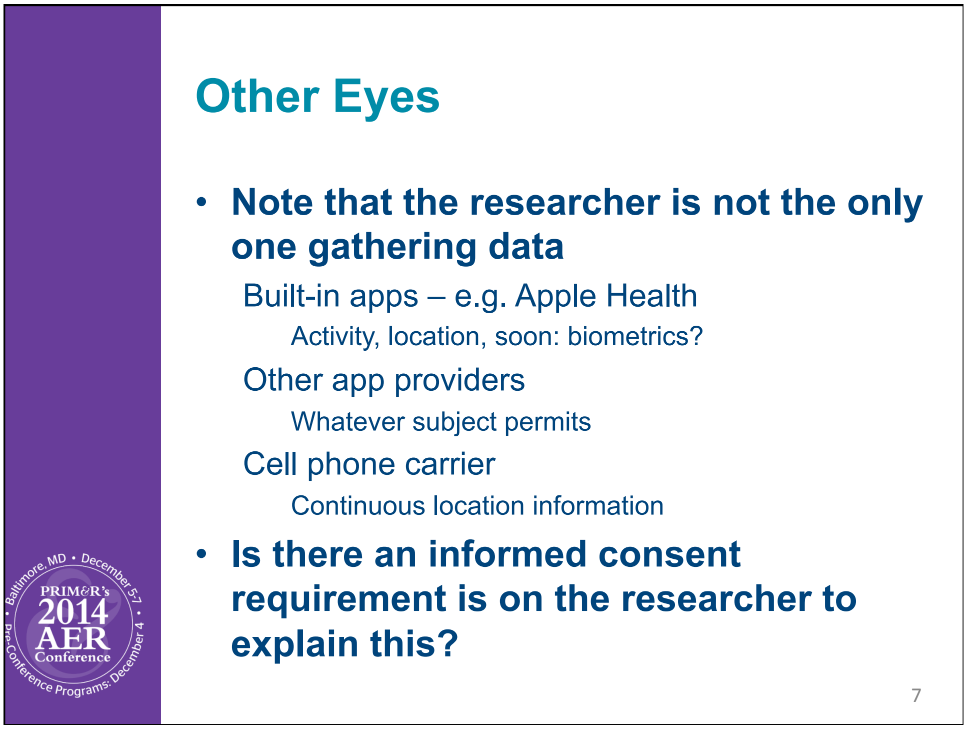
Smartphone as Tool

- **Obvious possibility**
  - Subject already has the data gathering tool
- **Today's smartphones are very powerful & very programmable**
- **Rich measurement capabilities**
- **Two edged sword**
  - Lots of interesting data available
    - Should only take data required for research
  - Privacy concerns
    - e.g., granularity of location data



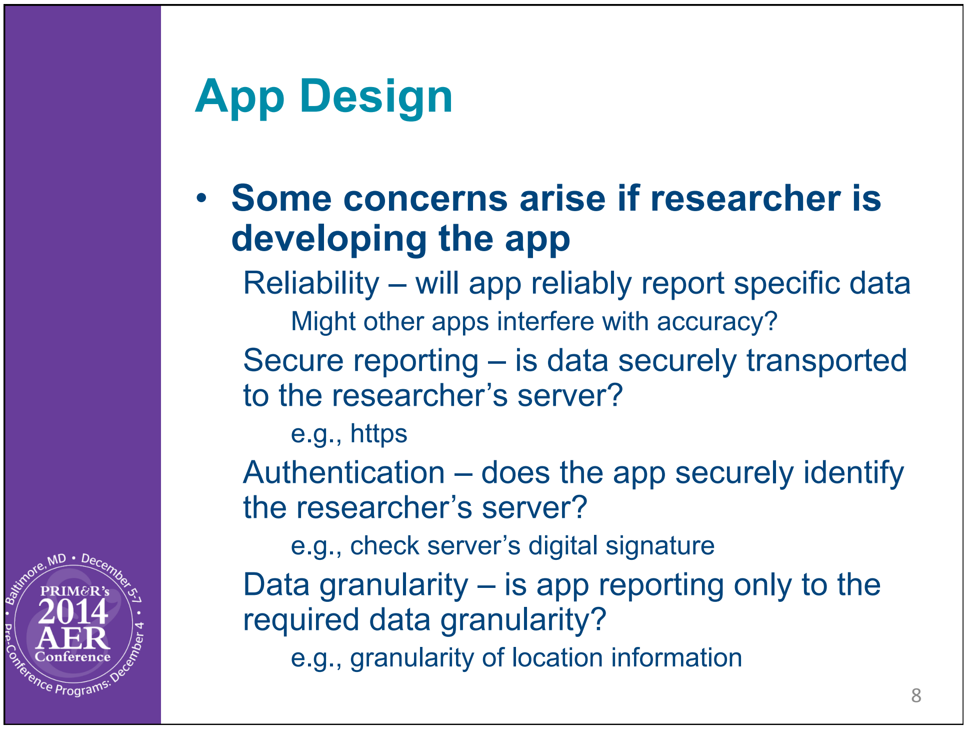
Protecting the Tool (BYORD)

- **Current generation smartphones can be easily well secured**
  - Just ask the FBI ☺
- **e.g., Harvard's iPhone requirements**
  - For all iPhones accessing Harvard systems
    - Personal or university owned
  - Use passcode (causes data to be encrypted)
  - Auto-wipe after 10 bad passcode tries
  - Enable Find my iPhone
  - Use encryption for email server access
- **Securing non-smartphones can be hard**
  - DYI security is generally not secure


Baltimore, MD • December 5-7 •
PRIM&R's
2014
AER
Conference
Pre-Conference Programs: December 4

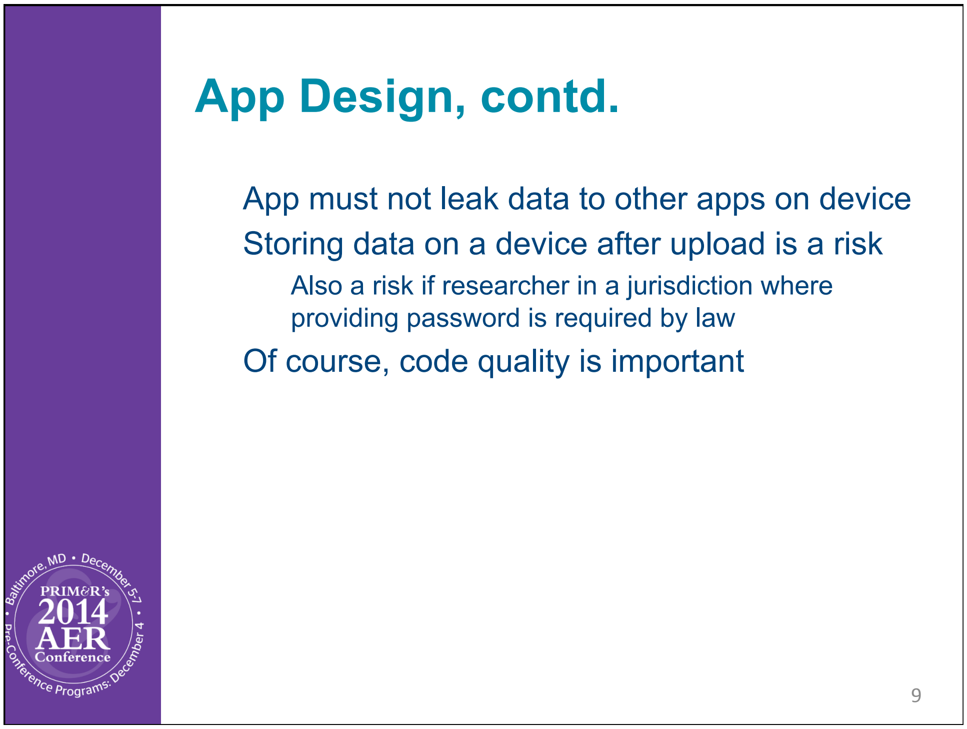
Other Eyes

- **Note that the researcher is not the only one gathering data**
  - Built-in apps – e.g. Apple Health
    - Activity, location, soon: biometrics?
  - Other app providers
    - Whatever subject permits
  - Cell phone carrier
    - Continuous location information
- **Is there an informed consent requirement is on the researcher to explain this?**


Baltimore, MD • December 5-7 •
PRIM&R's
2014
AER
Conference
Pre-Conference Programs: December 4

App Design

- **Some concerns arise if researcher is developing the app**
  - Reliability – will app reliably report specific data
    - Might other apps interfere with accuracy?
  - Secure reporting – is data securely transported to the researcher's server?
    - e.g., https
  - Authentication – does the app securely identify the researcher's server?
    - e.g., check server's digital signature
  - Data granularity – is app reporting only to the required data granularity?
    - e.g., granularity of location information



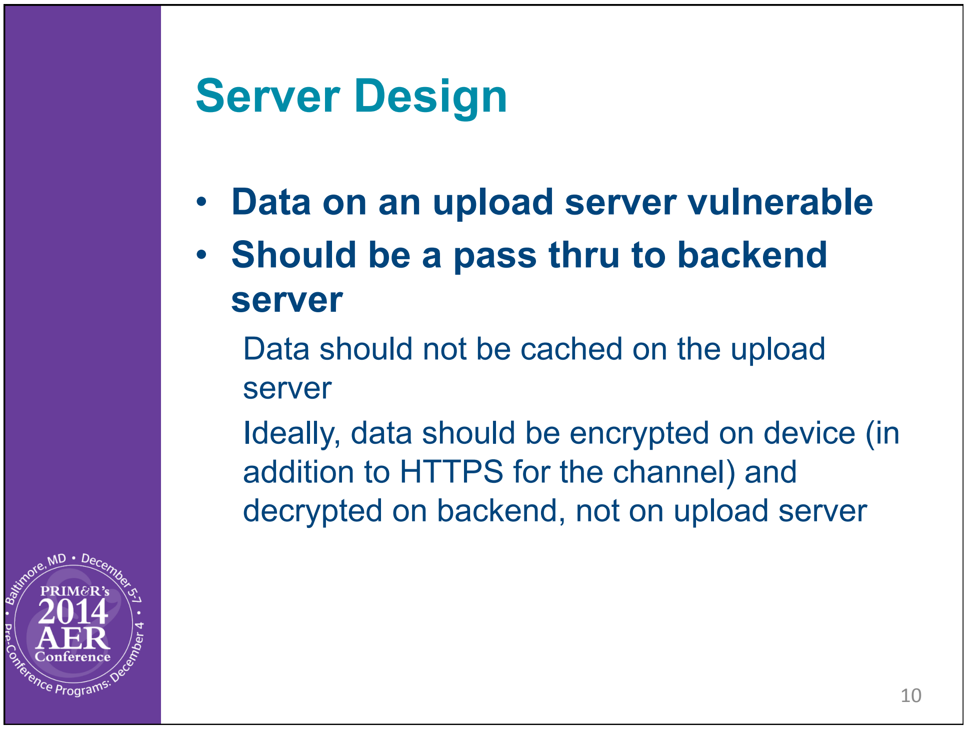
App Design, contd.

App must not leak data to other apps on device

Storing data on a device after upload is a risk

Also a risk if researcher in a jurisdiction where providing password is required by law

Of course, code quality is important

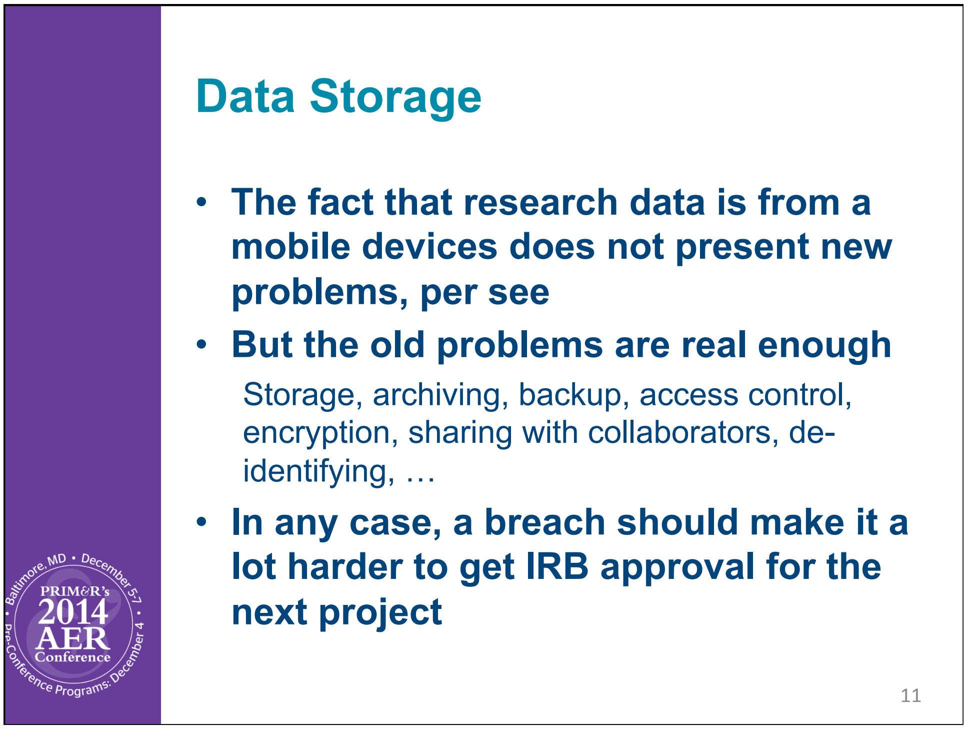


Server Design

- **Data on an upload server vulnerable**
- **Should be a pass thru to backend server**

Data should not be cached on the upload server

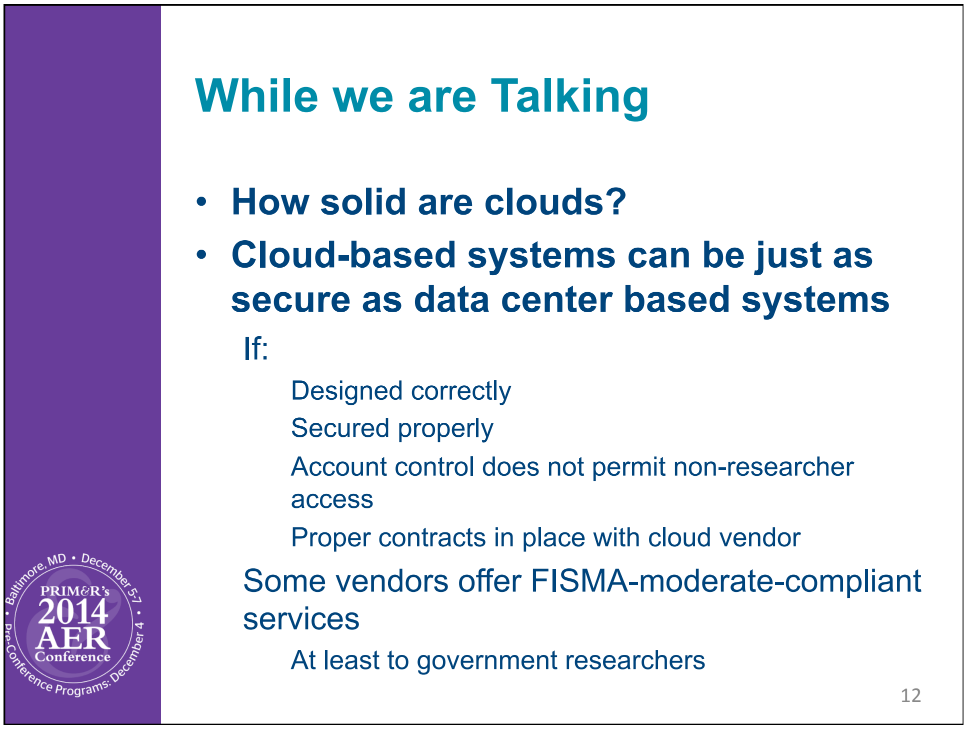
Ideally, data should be encrypted on device (in addition to HTTPS for the channel) and decrypted on backend, not on upload server



Data Storage

- **The fact that research data is from a mobile devices does not present new problems, per see**
- **But the old problems are real enough**

  Storage, archiving, backup, access control, encryption, sharing with collaborators, de-identifying, …
- **In any case, a breach should make it a lot harder to get IRB approval for the next project**

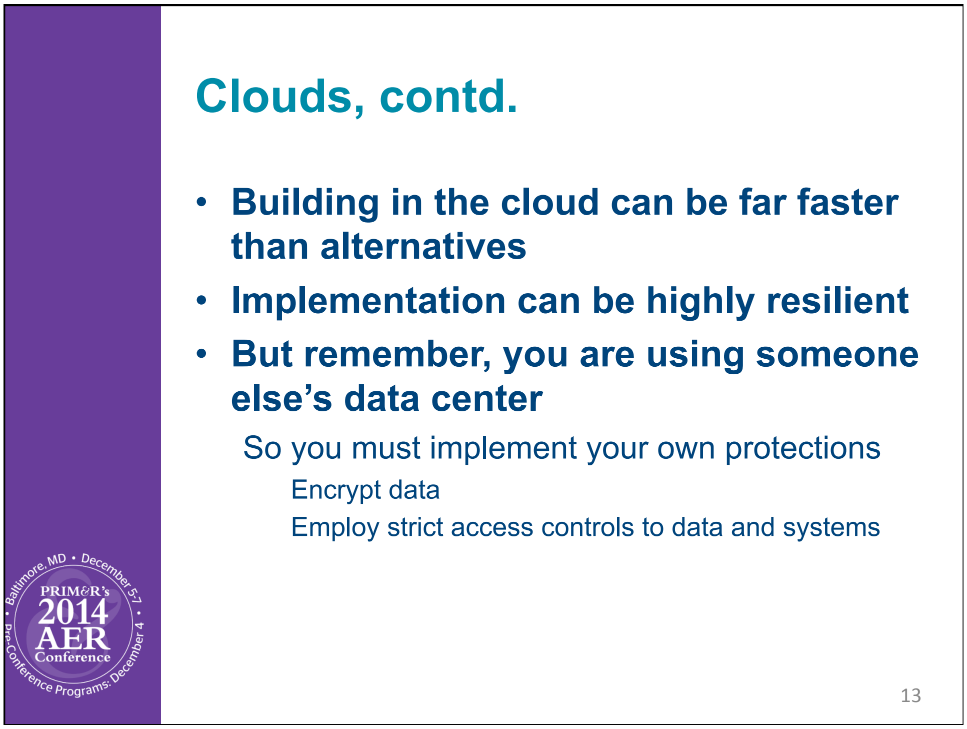


While we are Talking

- **How solid are clouds?**
- **Cloud-based systems can be just as secure as data center based systems**

  If:
  - Designed correctly
  - Secured properly
  - Account control does not permit non-researcher access
  - Proper contracts in place with cloud vendor

  Some vendors offer FISMA-moderate-compliant services
  - At least to government researchers

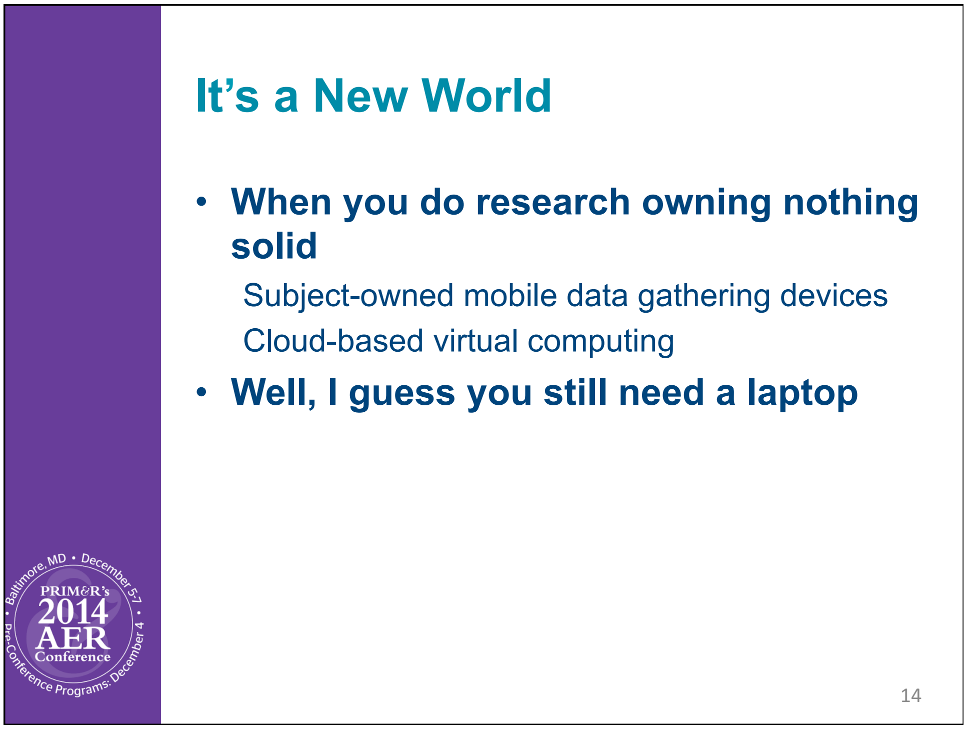


Clouds, contd.

- **Building in the cloud can be far faster than alternatives**
- **Implementation can be highly resilient**
- **But remember, you are using someone else's data center**
  - So you must implement your own protections
    - Encrypt data
    - Employ strict access controls to data and systems

Baltimore, MD • December 5-7 • PRIM&R's 2014 AER Conference • Pre-Conference Programs: December 4

13



It's a New World

- **When you do research owning nothing solid**
  - Subject-owned mobile data gathering devices
  - Cloud-based virtual computing
- **Well, I guess you still need a laptop**

Baltimore, MD • December 5-7 • PRIM&R's 2014 AER Conference • Pre-Conference Programs: December 4

14