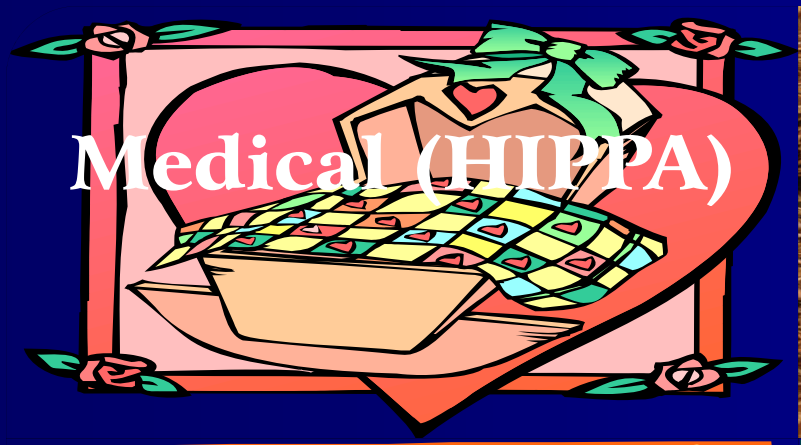
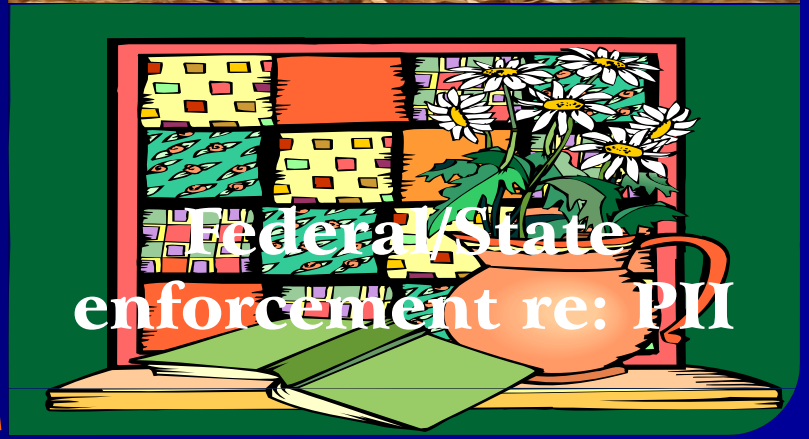
Personal Data Privacy in the United States

Ankur Kapoor
Constantine | Cannon LLP

September 15, 2012

The Patchwork Quilt





FTC Enforcement – PII

- § 5(a) of the FTC Act declares unlawful
  - "[u]nfair methods of competition"
  - "unfair or deceptive acts or practices"
- No misrepresentations re: data security & privacy

In re Facebook Allegations & Consent Order

- Facebook didn't meet its own, self-imposed obligations
  - Notwithstanding that some obligations went beyond what the law requires
- Consent Order
  - "establish and maintain a comprehensive privacy program"
- Google/Buzz

Apple GPS Tracking Class Action

- Tracking file on each "iDevice"
- Apple told consumers:
  - it would limit use of "personal information," including "data that can be used to uniquely identify or contact a single person."
- California's Consumer Legal Remedies Act and California's Unfair Competition Law

Apple GPS Tracking: No Invasion of Privacy

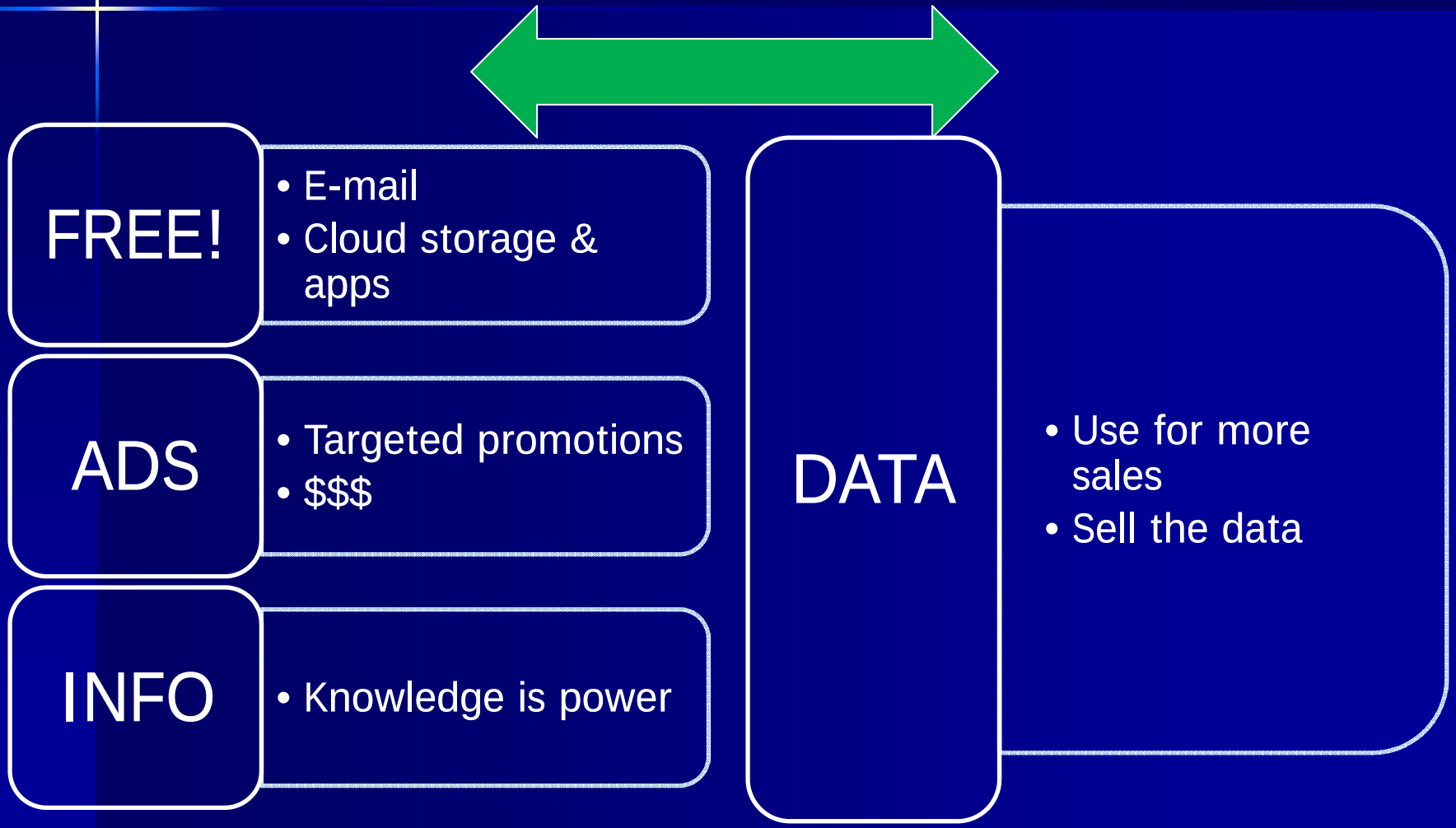
- Exists only for "egregious breach[es] of [] social norms," and Apple's alleged disclosure of personal information—even without users' knowledge or consent—was not so egregious but was "routine commercial behavior."

In re iPhone Application Litig., Case No.: 11-MD-02250-LHK (N.D. Cal. Jun. 12, 2012).

Why Unfair? The Deal

Consumers

Businesses



Why Unfair? The Deal

- The only currency that flows between consumer and business is DATA.
- Privacy policies are the terms of the deal.
- Also an element of competition

Best Practices in the U.S.: Data Privacy

- Clear, unambiguous, non-legalese statement of data privacy & security policies and practices – can link to a more detailed legal statement
- Disclose precisely what data are collected and how they are used – precise disclosure also makes it easier for your own employees to follow and monitor compliance
- Disclose precisely to which third parties or categories of third parties data may be disclosed – easier for compliance
- Access only data that the application needs
- Consent for every change

Best Practices in the U.S.: Data Security

- Permanent deletion when called for
- Take reasonable security measures: strong passwords; firewalls; encryption
- Regularly monitor security and keep updated
- If you've been hacked, find out exactly what happened and do everything you can to stop it from happening again
- Avoid putting large collections of personal data on portable media
- Require third parties to commit contractually to maintain the security of the data you give them

Best Practices in the U.S.: Compliance Infrastructure

- Designate a Chief Privacy Officer
  - Fully comprehend the flow of data to verify and monitor compliance
- Incorporate privacy and security policies and practices into existing internal mechanisms and procedures for contract compliance
- Train all employees

Remember Two Things

- Follow your own rules
- Don't make promises you're not sure you can keep

India

- "Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011"
- Promulgated pursuant to Information Technology Act of 2000

Indian Central Government's Ministry of Communications and Information Technology

India: Two Categories

- Personal information
  - "any information that relates to a natural person . . . capable of identifying such person"
- Sensitive personal data or information
  - any information comprising or "relating to":
    - passwords;
    - financial and payment information;
    - physical, physiological, and mental health;
    - medical records or history;
    - biometric information; and
    - sexual orientation.

India: Additional Requirements

- ID the purpose(s) of collection, use, sale, and transfer—and the recipients—while collecting
- Sensitive information: "consent in writing . . . before collection"
- Opt-out AND option to withdraw prior consent
- Consumer access and ability to amend data
- No transfer to third parties without consent and same protections as India

Questions