Get Security and Privacy Right

The views expressed are those of the speaker and not necessarily those of the FTC.

January 30, 2014
Laura D. Berger
Federal Trade Commission


myspace
GUESS
GUESS
ECHOMETRIX
nta
Path
RITE AID
facebook
cardsystems
the power of the right solution
compete
TOWER RECORDS
Tower.com
CVS
CAREMARK
ACRAnet
THE INFORMATION NETWORK
ScanScout
Settlement One
US SEARCH
BE INFORMED
Aaron's
RRS
Chitika
DAVE AND BUSTER'S
D&B
TRENDnet
epic
MARKETPLACE
Google
AMERICAN UNITED MORTGAGE COMPANY
DSW
twitter
Cbr
cord blood registry
ControlScan
Security that fits.
CARTMANAGER
PETCO
PL$
Sears
PREMIER Capital Lending
upromise
SAVE FOR COLLEGE
LexisNexis
GOAL FINANCIAL
Brightest Flashlight
Android App by GoldenShores Technologies, LLC
LOOKOUT
SERVICES
HOOKED ON PHONICS
htc
ValueClick
media
Lilly
CREDIT
SCS
REPORTING
LifeLock
CERIDIAN
Guidance
SOFTWARE
Life is good.
NRCUA
SUPERIOR MORTGAGE
BJ'S WHOLESALE CLUB
Where values come to life.
Come home to
James B. NUTTER & Company
Mortgage Lenders Since 1951
COMPUTER GEEKS.COM
Microsoft
T.J.maxx
ChoicePoint

Laws to keep in mind

- Section 5 of the FTC Act - broadly prohibits "unfair or deceptive acts or practices in or affecting commerce;
- COPPA – protects kids' data;
- GLB – protects financial data; and
- FCRA – protects data used for certain purposes (e.g., credit, hiring).

Common Remedies

- Injunction against misrepresentations
- Comprehensive data security or privacy program appropriate to the company's size, nature of activities, and information collected
- Third party assessments of these programs
- Other specific requirements, e.g., disclosures, privacy choices, data deletion, or software updates.
- Civil penalties for rule and order violations

Some Common Privacy Failures

- Rolling out a new service or feature that increases sharing without adequate notice and consent
- Misrepresenting with whom data is being shared
- Misrepresentations about tracking and opting out of tracking

Early Cases – Deception about Sharing

- Voluntarily submitted user data, disclosed to third parties for marketing, contrary to company promises.
- Geocites (1999) was our first internet privacy case. Involved sharing of member data with advertisers.
- ERCA and NRCUA (2003) involved student survey data.

Enforcement – Data Collection

- Path: App accessed contacts data, including of children, without authorization. Offered false choice in "Add Friends" feature.
- Upromise and Compete (privacy counts):
  - Toolbar collected extensive data, including financial data, passwords, and search terms.
  - Companies deceived users as to extent of data collection, akin to Sears case.

Enforcement - Sharing with Advertisers

- Facebook (1 of 8 counts) and Myspace
  - Both companies provided advertisers with information they said they would not share.
  - Leakage of user ID to advertisers allowed advertisers to identify users and link to web browsing, contrary to companies' claims.

Enforcement – Privacy Settings and Opt Outs

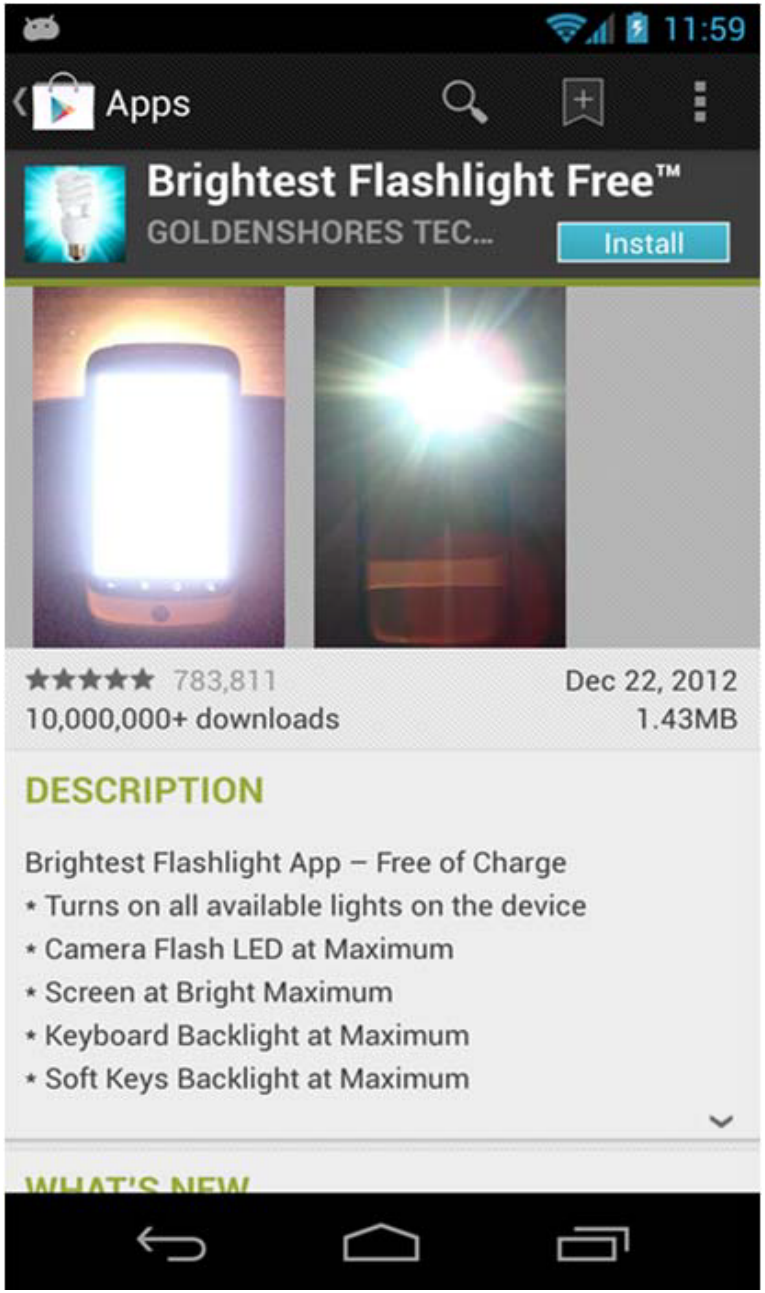
- Facebook: privacy settings misrepresented that users could restrict access to profile information to a selected audience.
- Twitter: privacy settings misrepresented that company would take at least reasonable steps to uphold the user's selection.
- Chitika: misrepresented that opt outs would last for a reasonable period of time.
- Google: options to decline Buzz didn't work.

Enforcement – Material Retroactive Change

- Facebook: Failed to get informed consent to apply changes to previously collected information. Alleged harm (e.g., risk of unwelcome contacts or revelation of potentially sensitive information to others).
- Gateway Learning: Applied material changes to previously collected information. First case to allege deception and unfairness re privacy changes.

Goldenshores

- Goldenshores' privacy policy stated that any information collected by the Brightest Flashlight app would be used by the company, and listed some categories of information that it might collect.
- The policy did not mention that the information would also be sent to third parties, such as advertising networks.
- Started transmitting data before consumer's could accept EULA



Information Security -- Four Points that Guide the FTC's Enforcement

- Information security is an ongoing process.
- A company's security procedures must be reasonable and appropriate in light of the circumstances.
- A breach does not necessarily show that a company failed to have reasonable security measures – there is no such thing as perfect security.
- Practices may be unreasonable and subject to FTC enforcement even without a known security breach.

Early Cases – Credit Card Data

Early Cases – Some Common Mistakes

- Storing information longer than needed or online when not necessary
- Using default or other easy-to-guess passwords
- Storing or transmitting information (including passwords!) in plain text
- Failing to take steps to segment or restrict access to data
- Failing to provide appropriate employee training and oversight
- Failing to take reasonable steps to detect or investigate breaches

More recent cases show

- Early mistakes continue to occur.
- New vulnerabilities may become “commonly known” (e.g., P2P software).

TRENDnet

- Security vulnerabilities in IP cameras and mobile apps could allow unauthorized access and control. A hacker accessed hundreds of camera feeds.
- TRENDnet: transmitted user login credentials in clear, readable text over the Internet; stored user login credentials in clear, readable text on user mobile devices; failed to implement a process to actively monitor security vulnerability reports; and failed to employ reasonable and appropriate security in the design and testing of the software that it provided consumers for its IP cameras.

TRENDnet – design and testing failures

- did not perform security review and testing of the software at key points, such as upon the release of a camera or the release of software for it, such as:
  - a security architecture review;
  - vulnerability and penetration testing of the software;
  - reasonable and appropriate code review and testing of the software.
- did not implement reasonable guidance or training for responsible employees.

TRENDnet-alleged deception

- Through its marketing statement and user interface, the Company represented that it had taken reasonable steps to ensure that (1) its cameras are a secure means to monitor private areas of a consumer's home or workplace and (2) that a user's security settings will be honored.

- Due to the Company's alleged security failures, these representations constitute false or misleading claims.

TRENDnet-alleged unfairness

- The company failed to provide reasonable security to prevent unauthorized access to live IP camera feeds.
- The alleged security failures caused, or are likely to cause, substantial injury to consumers that is not outweighed by benefits and is not reasonably avoidable by consumers.
- Potential harms from the exposure of sensitive information through the IP cameras included an increased likelihood that (1) consumers or their property will be targeted for theft or other criminal activity or that (2) consumers' personal activities and conversations or those of their family members, including young children, will be observed and recorded over the internet.

HTC

- Security vulnerabilities in handsets, including insecure implementation of logging applications, could permit malicious apps to send texts, record audio, and install additional malware.
- HTC failed to: provide adequate security training for engineers; review or test its mobile device software for potential security vulnerabilities; follow well-known and commonly accepted secure coding practices; and establish a process to receive and address vulnerability reports from third parties.

rockyou

- Gaming site failed to maintain reasonable data security and violated COPPA.
- Privacy policy promised “commercially reasonable efforts” for security, but company stored passwords in plain text.
- Hacker accessed the information of 32 million users, including children.

- P2P file sharing apps for desktop and Android
- Likely would cause consumers to unwittingly expose sensitive personal files stored on their mobile devices (“unfair design”).
- Misled consumers about which downloaded files from desktops and laptops would be shared.

FTC Advice for App Developers

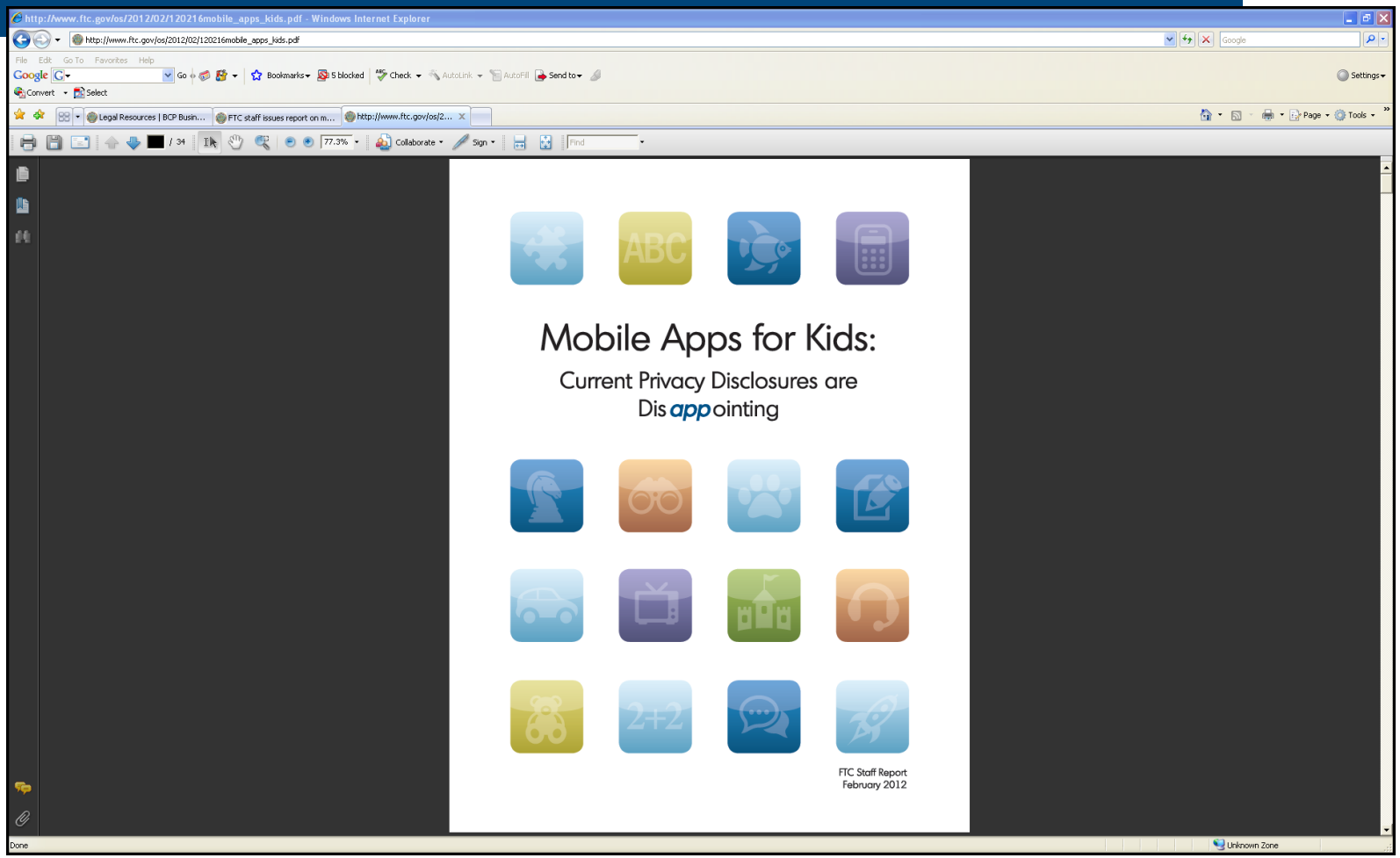
- Tell the truth about what your app can do.
- Disclose key information clearly and conspicuously.
- Build privacy considerations in from the start.
- Be transparent about your data practices.
- Offer easy to find and easy to use choices.
- Honor your privacy promises.
- Protect kids' privacy.
- Collect sensitive information only with consent.
- Keep user data secure.

Mobile App Developers: Start with Security

- Make someone responsible for security.
- Take stock (and practice minimization).
- Understand differences between mobile platforms.
- Don't rely on a platform alone to protect your users.
- Generate credentials securely.
- Use transit encryption for usernames, passwords, and other important data.
- Use due diligence on libraries and other third-party code.
- Consider protecting data you store on a user's device.
- Protect your servers, too.
- Don't store passwords in plaintext.
- You're not done once you release your app. Stay aware and communicate with your users.

Improving Your Disclosures

Kids App Survey



Kids Apps Survey

- Reviewed 200 kids apps on Android and 200 on Apple
- Looked for disclosures available in App stores or by developers
- Very little information disclosed prior to download
- Recommendation – app stores, developers and other ecosystem participants need to improve disclosures re data practices

Second Kids App Report

Second Kids App Report

- Little progress in giving parents information re what data is collected from kids, how it is shared, or who has access.
- Many apps sent data from the mobile device to ad networks, analytics companies, or other third parties, without disclosing these practices to parents.
- Recommendation - app stores, developers, and others ecosystem participants need to accelerate efforts to inform parents AND should implement recommendations in the recent FTC Privacy Report including:
  - privacy by design for mobile products and services;
  - easy-to-understand choices for parents; and
  - greater transparency about how data is collected, used, and shared.

- Questions?
- Lberger@ftc.gov