Privacy and Data Breach Issues

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

April 11, 2014
Laura D. Berger
Federal Trade Commission
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).
Some 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; and
- 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
- Presenting false choices
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.
Goldenshores

- Privacy policy stated that information collected by the app would be used by the company, and listed some categories of information that it might collect.
- Policy did not mention that data would be sent to third parties, such as ad networks.
- Started sending data – including geo and device ID -- before consumers could “Accept” or “Refuse” EULA.
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.
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.
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
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.
More recent cases show

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

MARKETING YOUR MOBILE APP
GET IT RIGHT FROM THE START
- 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.
Protecting Personal Information:
A Guide for Business

5 key principles:

1. Take stock. Know what personal information you have in your files and on your computers.

2. Scale down. Keep only what you need for your business.

3. Lock it. Protect the information that you keep.


5. Plan ahead. Create a plan to respond to security incidents.
Identify computers or servers where sensitive personal information is stored.

Identify all connections to these computers (e.g., Internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, digital copiers, and wireless devices like smartphones, tablets, or inventory scanners).

Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.
Protecting Personal Information – tips on General Network Security (2 of 3)

- Don’t store sensitive consumer data on a computer with an Internet connection unless it’s essential for your business.
- Encrypt sensitive data that you send to third parties over public networks (like the Internet), and consider encrypting sensitive data stored on your network or on portable storage devices. Consider encrypting emails within your business that contain personally identifying information.
- Regularly run up-to-date anti-virus and anti-spyware programs on your network.
Protecting Personal Information – tips on General Network Security (3 of 3)

- Check expert websites (e.g., www.sans.org) and software vendor websites regularly, and implement policies for installing vendor-approved patches.
- Consider restricting employees’ ability to download unauthorized software.
- Scan computers on your network to identify and profile the operating system and open network services. Disable services that you don’t need.
- When you receive or transmit credit card or other sensitive financial data, use Secure Sockets Layer (SSL) or another secure connection to protect it in transit.
Prioritizing Computer System Risks

- Check expert consensus lists that identify and offer defenses for the commonly exploited vulnerabilities that pose the greatest risk of harm to your information systems.
  - **The 10 Most Critical Web Application Security Vulnerabilities** ([www.owasp.org](http://www.owasp.org)) Describes common vulnerabilities for web apps and databases and the most effective ways to address them. These vulnerabilities are as important as network issues.

**Contractors and Service Providers**

- Before you outsource a business function (payroll, web hosting, data processing, etc.) investigate the company’s data security practices and compare their standards to yours. If possible, visit their facilities.

- Address security issues for the type of data your service providers handle in your contract with them.

- Insist that your service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of your data.
Incident response plans

- Have a plan to respond to security incidents. Designate a senior staff member to coordinate and implement the plan.
- If a computer is compromised, disconnect it immediately from your network.
- Investigate security incidents immediately and take steps to close off existing vulnerabilities or threats to personal information.
- Consider whom to notify in the event of an incident, both inside and outside your organization. You may need to notify consumers, law enforcement, customers, credit bureaus, and other businesses that may be affected by the breach. In addition, many states and the federal bank regulatory agencies have laws or guidelines addressing data breaches. Consult your attorney.
Visit www.business.ftc.gov for more information.

Questions?
Lberger@ftc.gov