Privacy at the Federal Trade Commission

Delhi, India – September 2013

Sarah Schroeder & Betsy Broder
US Federal Trade Commission

Overview of the FTC

- Nation's only general jurisdiction consumer protection agency
- Independent federal agency headquartered in Washington, DC with 7 regional offices
- Five Commissioners
- Enforcement through federal district court and administrative litigation

FTC's Approach to Privacy

- The FTC's standard is that companies must:
  - maintain reasonable procedures to protect sensitive consumer information, and
  - live up to any promises they make regarding the privacy or security of their information.


myspace
GUESS
ECHOMETRIX
nta
Path
RITE AID
facebook
cardsystems
the power of the right solution
compete
CVS
ACRAnet
ScanScout
SettlementOne
US SEARCH
BE INFORMED
CAREMARK
TOWER RECORDS
Tower.com
Chitika
DAVE AND BUSTER'S
D&B
epic
MARKETPLACE
RRS
Google
AMERICAN UNITED MORTGAGE COMPANY
DSW
twitter
Cbr
cord blood registry
ControlScan
Security that fits.
CARTMANAGER
PETCO
CREDIT
SCS
REPORTING
Sears
PREMIER Capital Lending
upromise
SAVE FOR COLLEGE
LexisNexis
GOAL FINANCIAL
HOOKED ON PHONICS
htc
ValueClick
media
NRCUA
LOOKOUT
SERVICES
LifeLock
CERIDIAN
Guidance
SOFTWARE
Lilly
Life is good.
PL$
SM
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

Overview of Laws

Federal Trade Commission Act (FTC Act)

Fair Credit Reporting Act (FCRA)

Gramm-Leach-Bliley Act (GLB Act)

Children's Online Privacy Protection Act (COPPA)

FTC Act - Deceptive Privacy & Security Claims

- The FTC has brought cases against companies that misrepresented their privacy & security procedures.

- Companies claimed to have strong procedures in place to protect the information they collected. In fact, the companies failed to anticipate or address substantial and well-known security risks.

Case Example:

- Provided privacy controls to users to keep private "tweets" and nonpublic user info – including mobile phone numbers – private
- Due to lapses in security, hackers obtained unauthorized administrative control of Twitter, accessed private info, and took over user accounts
- Order prohibits misrepresentations, requires reasonable security, and mandates independent, comprehensive security audits

FTC Act - Unfair Privacy & Security Practices

- The FTC has brought cases alleging that the failure to have reasonable security procedures was an unfair practice.

- In each case, as a result of the company's inadequate safeguards, there was a data breach that resulted in substantial consumer injury.

Case Example: T.J.maxx®

- Due to lax security methods, hackers stole tens of millions of consumer credit cards, resulting in tens of millions in fraudulent charges.
  - Stored personal information on, and transmitted it between and within, in-store and corporate networks in clear text;
  - Did not limit wireless access to its networks, allowing an intruder to connect wirelessly to in-store networks without authorization;
  - Did not require strong passwords;
  - Failed to limit access among computers and the internet, such as by using a firewall; and
  - Failed to detect and prevent unauthorized access to computer networks or to conduct security investigations, such as by patching or updating anti-virus software or following up on security warnings and intrusion alerts.

Case Example: facebook

- FTC alleged (among other things):
  - unfair to override users' privacy settings
  - privacy settings were deceptive if they didn't do what a reasonable consumer thought they would
  - Misrepresented applications' access to data
  - didn't live up to promises about deleting users' info
- Significant Settlement Terms:
  - required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences;
  - required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account
  - Requires the company to adopt a comprehensive privacy program

Fair Credit Reporting Act (FCRA)

- Credit transactions are extremely common in the U.S.
- Consumer Reporting Agencies collect public record info, credit info, both positive and negative
- The information is sensitive and subject to strict privacy protections under the FCRA
- FCRA requires CRAs to maintain reasonable procedures to ensure that users have a permissible purpose to access records

Case Example:

- The FTC alleged that ChoicePoint failed to use reasonable procedures to screen prospective subscribers and monitor their access to sensitive consumer data
- These failures allowed identity thieves posing as legitimate businesses to obtain access to the personal information of many consumers
- At least 800 cases of identity theft arose out of these incidents.
- Record $10 million civil penalty for violations of the FCRA
- $5 million in consumer redress for identity theft victims

Gramm-Leach-Bliley Act – Safeguards Rule

Rule Requires:

- Financial institutions to develop and implement appropriate physical, technical, and procedural safeguards to protect customer information.

Elements:

- Written information security plan
- Designate employee(s) to coordinate safeguards
- Identify and assess risks to customer information
- Oversee service providers
- Periodically update information security program

Case Example:

- Nations Title Agency
- Promised consumers the company would protect their confidential financial information
- Tossed consumers' home loan applications in an open dumpster

Outsourcing

- Businesses subject to U.S. laws that outsource personal information retain responsibility for ensuring that there are reasonable procedures in place to safeguard that information.
  - This responsibility is the same whether the service provider is located within the U.S. or offshore.

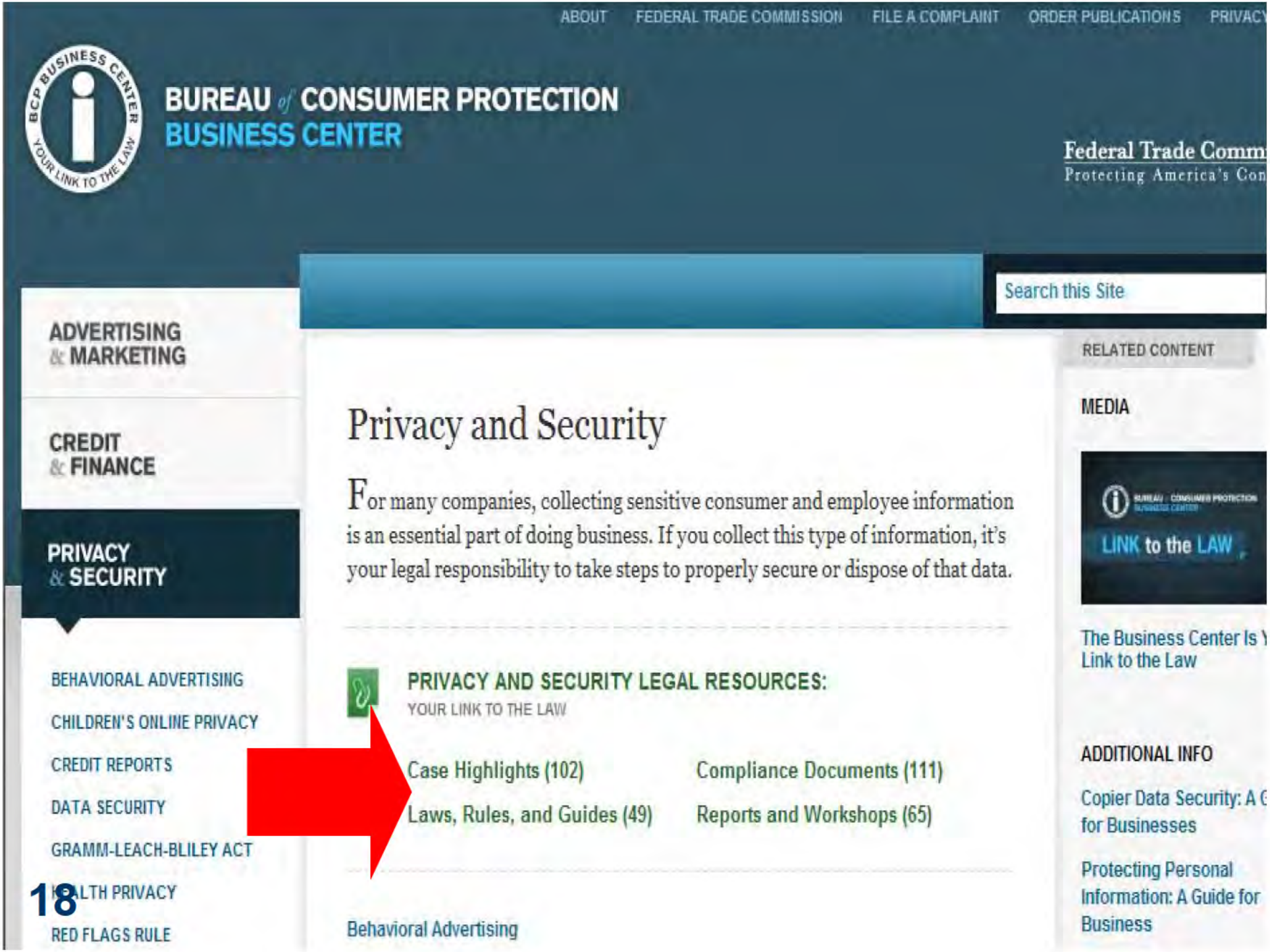
Children's Online Privacy Protection Act

- COPPA is the only child-specific federal privacy law in the United States.

- Among other things, operators of commercial websites and online services must provide NOTICE and obtain parents' CONSENT before collecting personal information from children under age 13.

Case Example: Artist Arena

- FTC sued operator of fan websites for music stars Justin Bieber, Rihanna, Demi Lovato, and Selena Gomez.
- Children were able to register to join a fan club, create profiles and post on members' walls.
- Complaint alleged that Artist Arena knowingly registered 25,000 children under age 13 without parental consent.
- $1 million civil penalty.


ABOUT
FEDERAL TRADE COMMISSION
FILE A COMPLAINT
ORDER PUBLICATIONS
PRIVACY
BCP BUSINESS CENTER
YOUR LINK TO THE LAW
BUREAU of CONSUMER PROTECTION
BUSINESS CENTER
Federal Trade Comm
Protecting America's Con
Search this Site
ADVERTISING & MARKETING
CREDIT & FINANCE
PRIVACY & SECURITY
BEHAVIORAL ADVERTISING
CHILDREN'S ONLINE PRIVACY
CREDIT REPORTS
DATA SECURITY
GRAMM-LEACH-BLILEY ACT
HEALTH PRIVACY
RED FLAGS RULE
Privacy and Security
For many companies, collecting sensitive consumer and employee information is an essential part of doing business. If you collect this type of information, it's your legal responsibility to take steps to properly secure or dispose of that data.
PRIVACY AND SECURITY LEGAL RESOURCES:
YOUR LINK TO THE LAW
Case Highlights (102)
Compliance Documents (111)
Laws, Rules, and Guides (49)
Reports and Workshops (65)
Behavioral Advertising
RELATED CONTENT
MEDIA
LINK to the LAW
The Business Center Is Y
Link to the Law
ADDITIONAL INFO
Copier Data Security: A G
for Businesses
Protecting Personal Information: A Guide for Business

Questions?

- More information available at:

  www.ftc.gov

Sarah Schroeder
sschroeder@ftc.gov
Federal Trade Commission

The views expressed are those of the speaker
and not necessarily those of the FTC or any other person.