ITECHLAW™
INTERNATIONAL TECHNOLOGY LAW ASSOCIATION

Hot Topics in Privacy Law

The FTC's Proposed New Framework

Alan N. Sutin
Chair, Global Intellectual Property & Technology Practice, Greenberg Traurig LLP
New York, NY

Introduction

- Overview of FTC Preliminary Report
- Discussion of newly emerging privacy framework
- Focus on location data – a new addition to the class of “sensitive” information

Regulation of Privacy in the U.S.

- Patchwork quilt of state and federal laws
- Existing Federal laws and regulations largely cover specific types of data relating to money, health or children (e.g., GLB, HIPAA, FCRA, COPPA)
- About a decade ago the FTC began bringing enforcement actions in the privacy context using its authority under Section 5 of the FTC Act.
  - Initial focus was on deceptive acts inconsistent with representations made in a company's privacy notice

History of FTC Enforcement

- Since about 2005, the FTC began to expand its jurisdiction in the privacy and information security context, and began to focus on information security breaches using the “unfairness” prong of Section 5
  - **Coincided with proliferation of state breach notification laws**
  - **The FTC began asserting that a data security breach, even without a deceptive representation, could constitute an unfair trade practice under Section 5, and used this theory in enforcement actions resulting from breaches (e.g., BJ’s, ChoicePoint, CardSystems, DSW, TJX, etc.)**

ITECHLAW™
INTERNATIONAL TECHNOLOGY LAW ASSOCIATION

FTC Preliminary Report -- December 1, 2010

Protecting Consumer Privacy in an Era of Rapid Change

A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS

FTC Report: Overview

- "Privacy by Design"
  - Incorporate Fair Information Practice Principles (notice, choice, access, security and enforcement) into everyday practices
  - Maintain comprehensive data management procedures throughout the life cycle of products and services
- Simplified consumer choice
  - Inferred consent for "commonly accepted practices"
  - Offer "informed and meaningful choice" for all other practices
  - Support for "Do Not Track" mechanism

FTC Report: Overview

- Greater transparency
  - Clearer, shorter, standardized privacy policies
  - Reasonable access to information
  - Robust notice and express consent for material changes applied retroactively
  - Consumer education

FTC Report: Privacy By Design

- Adopt a “privacy by design" by building Fair Information Practices into everyday business operations, including:
  - Provide reasonable security for consumer data;
  - Collect only the data needed for a specific business purpose;
  - Retain data only as long as necessary to fulfill that purpose;
  - Safely dispose of data no longer being used; and
  - Implement reasonable procedures to promote data accuracy.

FTC Report: Privacy by Design

- **Companies should implement and enforce procedurally sound privacy practices throughout their organizations, including:**
  - Assigning personnel to oversee privacy issues,
  - Training employees on privacy issues, and
  - Conducting privacy reviews when developing new products and services.

FTC Report: Simplified Choice

- **Companies should provide choices to consumers about their data practices in a simpler, more streamlined way than has been used in the past.**
- **Inferred Consent for Obvious Practices:**
  - The FTC believes that it is reasonable for companies to engage in certain commonly accepted or obvious practices where consent is properly inferred – namely, product and service fulfillment, internal operations such as improving services offered, fraud prevention, legal compliance, and first-party marketing. It is not clear -- and comments will need to focus on -- what types of practices are obvious or commonly accepted.

FTC Report: Simplified Choice

- **Companies should provide choices to consumers about their data practices in a simpler, more streamlined manner.**
- **Inferred consent for obvious practices:**
  - It is reasonable for companies to engage in certain commonly accepted or obvious practices where *consent is properly* inferred. Examples include:
    - product and service fulfillment
    - internal operations such as improving services offered
    - fraud prevention
    - legal compliance
    - first-party marketing

FTC Report: Simplified Choice

- No Inferred Consent Where Practices Are Not Obvious:
  - For data practices that are not “commonly accepted,” consumers should be able to make informed and meaningful choices.
  - Choices should be clearly and concisely described and offered – and at the point the consumer is making a decision about his or her data.
- Support for Do Not Track
  - The FTC staff supports a universal choice that would likely involve the placement of a persistent setting, similar to a cookie, on the consumer’s browser signaling the consumer’s choices about being tracked and receiving targeted ads.

FTC Report: Transparency

- Companies should make their data practices more transparent to consumers.
  - Improve their privacy policies and make them more consistent and easier to read so parties can better compare data practices and choices.
  - Provide consumers with reasonable access to the data that companies maintain about them, *particularly for companies that do not interact with consumers directly, such as data brokers*.
  - The extent of access should be proportional to both the sensitivity of the data and its intended use.
  - All entities must provide robust notice and obtain affirmative consent for material, retroactive changes to data policies.

FTC Report: Concurring Opinions

- Commissioner Kovacic
  - Calls Do Not Track proposal “premature”
  - Limiting firms advertising abilities may reduce revenue and degrade quality
  - Wants more context about existing privacy framework and how protection is inadequate

FTC Report: Concurring Opinions

- Commissioner Rosch
  - Enhance efforts to enforce the “notice and choice” model, rather than replace it
  - Require notices to be clear, conspicuous and effective
  - Consumers should opt in to Do Not Track mechanism

FTC Report: Questions for Comment

- Report poses 5 pages of questions for comment
- Addresses how each component of the proposed framework might apply in the real world
- Commission staff seeks comment by February 28, 2011
- Commission will issue a final report in 2011

FTC Report: Commerce Dept Report

- The Department of Commerce issued a "green paper" on privacy on Dec. 16, 2010
- Major themes:
  - Enforceable codes of conduct based on FIPPs
  - National data breach notification law
  - Privacy Policy Office in the DOC
  - More reliance on cooperative industry self-regulation
  - Recommends the FTC remain the lead consumer privacy enforcement agency for the U.S. Government

Location Data

- How many ways are we located every day?
  - When we carry cell phone turned on.
  - When we use our laptop computers in hotel.
  - When we charge things to our credit card.
  - When we use the ATM machine.
  - When we drive through monitored intersection.
  - When we past a security camera at the store.
  - When we scan our ID card to enter a building or room.

Multiplicity of devices, applications and networks collecting location data

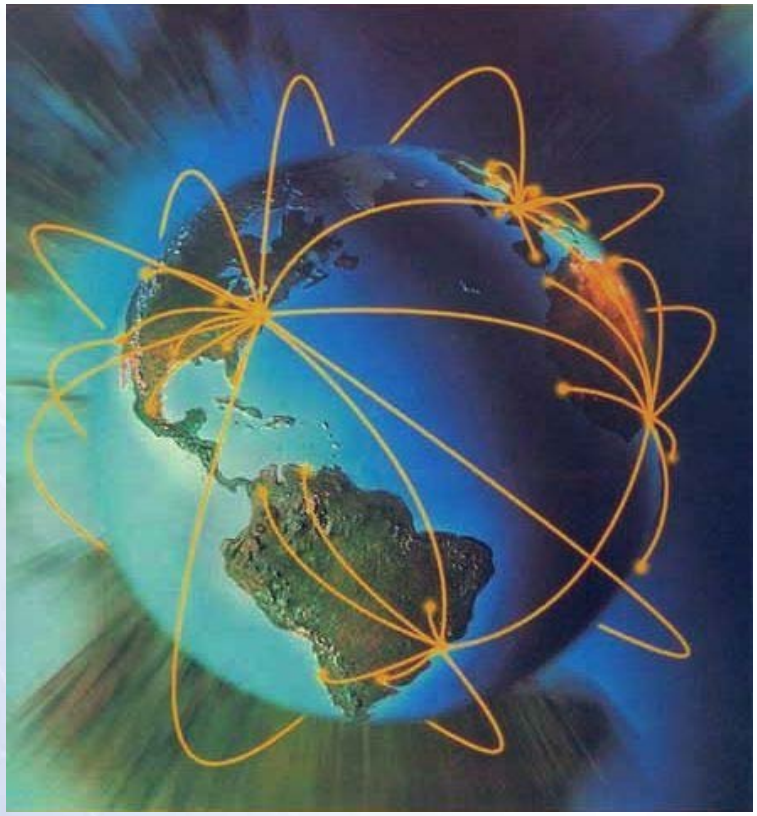
What uses are being made of location data

- Government uses
  - Investigation
  - Evidence
- Commercial Uses
  - Telecom services
  - Navigation
  - Directories
  - Targeted advertising


THE WALL STREET JOURNAL.
Finding the Holy Grail of Web Advertising
BtoB
THE MAGAZINE FOR MARKETING STRATEGISTS
Behavioral Targeting Grows
Los Angeles Times
Marketing Works by Targeting Consumers
DOWJONES
Online Marketing's New Tack
BUSINESS 2.0
MAGAZINE
The Quest for the Perfect Online Ad
THE WALL STREET JOURNAL.
How Marketers Hone Their Aim Online
The New York Times
Online Customized Ads Move a Step Closer
AdvertisingAge
Today's Niche Marketing is About Narrow, Not Small

United States Constitution

- United States Constitution
  - 4th Amendment: default standard governing evidence collection in criminal investigations
  - Technology raises new issues in 4th Amendment analysis



United States Constitution

- Fourth Amendment
  - Bans only "unreasonable" searches and seizures
  - Searches and seizures are "reasonable" if authorized by a warrant or a warrant exception
  - 4th Amendment is not implicated if there is no
    - Search
    - Seizure

United States Constitution

- GPS Tracking
  - court decisions inconsistent, but trend is to require warrant
- Recently:
  - NY court rules that GPS tracking is a constitutional "search" that requires a warrant.
  - MA court rules warrant required for GPS tracking

Location Data and CPNI

- The Communications Act and CPNI
  - *Who is Subject to Rules?*
    - Telecom carriers
      - Includes interconnected VoIP providers
  - The Telephone Records and Privacy Protection Act of 2006 ("TRPPA") is a generally applicable criminal statute
  - *What activities and information are covered?*
    - The collection and use of customer proprietary information by carriers, their partners and contractors.
    - When does location information qualify as CPNI?

Location Data and CPNI

- CPNI
  - *What are the key FCC rules relating to CPNI?*
    - Carriers may only use CPNI to provide requested services to the customer, or as authorized/directed by customer in writing
    - Customer info can be used in aggregate form
  - *What are the key rules under TRPPA?*
    - Unlawful to obtain CPNI from a carrier without authorization or using fraudulent means
    - May not Knowingly sell or transfer CPNI obtained improperly

Proposed New Federal Privacy Law

- SEC. 6. USE OF LOCATION-BASED INFORMATION. (a) IN GENERAL.—[Subject to limited exceptions], “any provider of a product or service that uses location-based information shall not disclose such location- based information concerning the user of such product or service without that user’s express opt-in consent. A user’s express opt-in consent to an application provider that relies on a platform offered by a commercial mobile service provider shall satisfy the requirements of this subsection.”
- (b) AMENDMENT.—Section 222(h) of the Communications Act of 1934 amended to add the following definition: ‘‘(8) CALL LOCATION INFORMATION.—The term ‘call location information’ means any location-based information.’’

ITECHLAW™
INTERNATIONAL TECHNOLOGY LAW ASSOCIATION

Thank You!

Alan N. Sutin
Chair, Global Intellectual Property &
Technology Practice

ITECHLAW™
INTERNATIONAL TECHNOLOGY LAW ASSOCIATION

Privacy, Data Protection and Social Networks

Naomi Assia & Co. – Law Offices, Patent Attorney's and Notary

•Over the last 4 years, the use of global cyber social networks increased tremendously.

•People keep personal content online, increasingly interact online, socially and professionally.

•Major privacy implications need to be considered.

According to NumberOf.net there are:

- 75 million users of Twitter 
- 500 million users of Facebook 
- 65 million users of LinkedIn. 
- Over 100 million users of MySpace. 

ISRAEL

According to comScore research Israel is in the 2nd place in the world for being the most active internet users in cyber social networks.

In the 1st place – Russia with 74.5% of the its total internet users which are the most active in social networks services with an average time of 9.8 hours per month (!!!) of each user which is using those social networks

Israel – an average of 9.2 hours per month of each user using social networks, mainly Facebook.

Social Networks Services allow the users to:

- Join to communities with similar fields of interests.
- Keep and share photos on the web.
- Get to know other users.
- Keep in touch with friends and family
- Play games with/against other users.
- Express political and social views.
- Advertize their business.

The main concerns in regard to the use of SNS (Social Networks Services)

- Protection of minors and data privacy
- The boundary between private and public areas
- Data protection and data trade
- Enforcement of Privacy Laws and international cooperation.

ITECHLAW™
INTERNATIONAL TECHNOLOGY LAW ASSOCIATION

Protection of **minors** and data privacy

Exposure to Illegal content

Identity theft

Propaganda

Sexual abuse/Sexual harassment

Gambling

Conduct

Actions taken by the EU:

Opinion 5/2009 on Online Social Networking of the Article 29 Data Protection Working Party (adopted June 12th 2009):

- Increase the awareness of minors
- Fair processing of the data submitted by the minor
- Implementation of new privacy protection technologies
- Providers self-regulation
- Legislative measures discouraging deception.

Safer Social Networking Principles (February 10th 2010)

- Raise awareness of safety education acceptable use policies.
- Ensuring services to be age appropriate.
- Tools to report inappropriate content and respond to reports.
- Assess means for reviewing illegal content / conduct.

United States – The legal framework

COPA (Child Online Protection Act – 1998)

- The purpose of the Act is to prohibit online sites from knowingly making available to minors material that is "harmful to minors"
- The law also created a temporary Commission to study various technological tools and methods for protecting minors from "material that is harmful to minors."

United States – The legal framework

Settlements between a coalition of all US State Attorneys (except Texas) and Myspace and Facebook in 2008 included:

- Implementation on design and functionality changes to the site
- Development of education and parental tools
- Collaboration of Myspace in detecting criminal acts of misusing the web
- Development of new privacy protection standards.
- Managing a registry of e-mail addresses provided by parents in order to restrict their children's access to a website.
- Improving the age verification process.
- Changes to the default privacy level settings for users under the age of 18

Israel – The legal framework

- **Basic Law – Human Dignity and Liberty**
  - The right for privacy recognized in Israel as a “basic right,” which equals to a constitutional right
- **Protection of Privacy Law – 1981 (“the Law”)**
  - All privacy issues and data protection issues are being dealt within the Law and the Law’s regulations
  - The Law determines high administrative fines and Statutory damages
  - Complaint is to be filed by the data subject, competitors or by ILITA, the Israeli Law, Information and Technology Authority
- **The Communication Act – 1982 and the amendment to the law of 2008**
  - Provisions for sending unauthorized messages (the Spam Act)
  - Opt-in mechanism for subscription to marketing/advertising materials
  - Administrative fines and statutory damages to the recipient

Global Privacy Enforcement Network (GPEN)

- 12 leading privacy protection authorities established an international entity to join efforts enforcing Privacy Protection laws.
- The countries which are members in GPEN: Israel, USA, Canada, France, New-Zealand, Australia, Ireland, England, Italy, Netherlands, Germany and Spain.
- It is critical that world-wide governmental authorities will join forces to increase their abilities to cooperate to enforce privacy protection regimes.
- Private information and data submitted to the web is being kept on servers located in various countries.
- Getting prepared to the “cloud computing” services.
- Transferring personal data in between various countries

Employer – Employee and SNS

- Fading boundaries between private and public correspondences:
  - Dismissal of employees following Facebook postings
  - Wall posting judged as private correspondence by the US court (Crispin V's Christian Audigier Inc)
  - Private information can be accessed in preliminary checkups.
  - The head of MI6 (Britain's Intelligence Service) personal details revealed over Facebook.
  - Employee established his own competing business, uploading his employer's contacts to his Linked-In account, shortly before terminating his employment.

Statistics:

- More than 500 million active users.
- Average user has 130 friends.
- People spending over 700 billion minutes per month on Facebook.
- There are 900 million objects that people interact with (pages, groups, events and community pages.
- Average user is connected to 80 community pages, groups and events
- Average user creates 90 pieces of content each month.
- More than 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums etc')
- More than 70 translations available on the site.
- About 70% of Facebook users are outside the USA.
- Entrepreneurs and developers from more than 190 countries build with Facebook platform.
- People on Facebook install 20 million applications every day.
- Every month, more than 250 million people engage with Facebook on external websites.
- 200 million users accessing Facebook from their mobile devices.

facebook

- Facebook's founder, Mark Zuckerberg says: "**The age of privacy is over."**
- People are sharing all personal information with other users in various web services, according to the level of privacy which they have chosen.
- People have gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.
- Privacy issues are being controlled by the users according to their preferences.
- According to Zuckerberg: **"The Facebook system is to reflect the current social norms are."**

Facebook in Israel:

• Number of users increased from 45,000 in September 2007 to 3.3 million in October 2010.

• 500,000 users accessing Facebook from their mobile devices.

• 34% of the Facebook users are “checking in” few times a day, 22% are having the Facebook web site open in front of them most of the day and 15% of the users are “checking in” once a day.

• 29% of Facebook users spend at least two hours on site. 26% spend 1 hour or so, 25% spend approx 30 min.

• In Israel the average Facebook user gain 232 friends (were the global average user gain 130 friends)

Facebook and Politics

Randi Zuckerberg, marketing director at Facebook said, in the DLD (Digital – Life – Design) Conference which is taking place these days in Munich that Facebook is interested to collect from its users' information, which will assist in understanding global conflicts.

Facebook wants to leverage its popularity (500 million users), in order to promote political and social agendas.

Facebook cooperates with universities and research institutions to process the data which is being stored on its servers in order to have perception on confrontations and political disputes around the globe,

Just recently, in the civil revolution which took place in Tunisa, Facebook became a major player in spreading the videos which were taken by the people on the street and their murmurings.

The phenomena became so broad that the Tunisian authorities have started to “hack” into the Facebook servers and delete accounts of Tunisian activists and other users which considered as a threat to the regime.

ITECHLAW™
INTERNATIONAL TECHNOLOGY LAW ASSOCIATION

eToro is the world's largest investment network, with over 1.5 million users in over 130 countries and over 2,000 new accounts opened each day. eToro leads the social trading revolution through its community powered network, which enables every investor to see, follow and copy the actions of other investors in real time. eToro's mission is to open the financial markets to every individual and make them accessible through a simple, transparent and more enjoyable way to trade currencies, commodities and indices online

eToro OpenBook:

OpenBook is a one of a kind social trading network that transforms the way people trade and invest online.

By enabling you to follow and interact with all other traders of the eToro community, OpenBook accelerates knowledge sharing and shortens the learning curve for you to bring your trading experience to the next level.

The followed subjects on OpenBook wave their right for total privacy, by allowing other users to follow their positions on the markets.

The “right to be forgotten”

- Digital “right to be forgotten” has been fixed by article 12 of the EU Directive 95/46, stating that member states shall guarantee every data subject the right to obtain from the data controller the deletion of the data.

- This essential legal tool faces difficulties to obtain complete deletion of profiles in SNS

- Facebook privacy policy clearly states that “when you deactivate your account, no user will be able to see it, but it will not be deleted. We save your profile information (connections, photos, etc’) in case you later decide to reactivate your account.”

The “right to be forgotten”

- New French bill that would impose new data breach obligations as well as strengthen the sanctioning power of the data protection authority:
  - Facilitate data subjects’ ability to request deletion of personal data.
  - Increase sanctioning powers and allow privacy violations victims to sue at their own local court houses instead of being obliged to sue in the court where the data controller is located.

- On October 13th 2010, the French digital minister has successfully brought together a dozen of social networking and search engines representatives to sign a charter for digital right to be forgotten

The “right to be forgotten”

- In the USA, the FTC and Congress have been pressing for new regulations that would deal with personal data deletion:
  - May 2010 - a proposition of a bill to require notice to and consent of individuals prior to the collection and disclosure of personal information
  - July 2010 – new bill (HR 5777) to foster transparency about commercial use of personal information.

Privacy Protection Breach Examples:

- Facebook – the “Wall Street Journal” revealed a data protection security breach when applications manufacturers transfer personal data from the users profiles to advertizing and survey companies, including information of the users’ friends.
- Israel - Personal details from the voters registry was used for commercial purposes.
- Israel - The city hall of Ramat Gan was fined for submitting personal data of high school students to a commercial company which promote courses.
- Israel - Direct mailing company was caught using the population registry database for commercial purposes.

Suggested solutions for effective data protection and privacy on SNS

- Review the regulatory framework on an international level.
- Transparency of data handling practices.
- Education of the users.
- Personal control of the data and shared information
- IT policies in companies towards employees.

Conclusions

- NO PRIVACY ON THE INTERNET !
- On the users side: all submitted data by the users can become public domain, thus, users should consider this assumption to begin with.
- On the SNS side: to increase the users faith in SNS Privacy policies.
- To increase global cooperation enforcing privacy acts and data protection policies.

THANK YOU

נעמי אסיא ושות' משרד עורכי דין,
עורכי פטנטים ונוטריון
Naomi Assia & Co. Law Offices
Patent Attorneys and Notary

רחוב הברזל 32, רמת החייל, תל-אביב 69710
32 Habarzel St., Ramat-Hachayal, Tel-Aviv 69710, Israel
Fax: 972-3-6444818 פקס: Tel: 972-3-6444808 טל:
Email: assia@computer-law.co.il • www.computer-law.co.il