When Past Performance May Be Indicative of Future Results

Legal Implications of Using Location-Based Services Data to Predict Future Behavior

Cyberspace Law Institute & Winter Working Meeting
January 31 - February 1, 2014
Denver, CO

Bruce Antley
Assistant General Counsel, AOL Inc.

Jason Haislmaier
Partner, Bryan Cave LLP
This presentation is intended for general informational purposes only and should not be construed as legal advice or legal opinion on any specific facts or circumstances, nor is it intended to address specific legal compliance issues that may arise in particular circumstances. Please consult counsel concerning your own situation and any specific legal questions you may have.

The thoughts and opinions expressed in this presentation are those of the individual presenters and do not necessarily reflect the official or unofficial thoughts or opinions of their employers.

For further information regarding this presentation, please contact the presenter(s) listed in the presentation.

Unless otherwise noted, all original content in this presentation is licensed under the Creative Commons Creative Commons Attribution-Share Alike 3.0 United States License available at: http://creativecommons.org/licenses/by-sa/3.0/us.
Outline

Overview
Privacy
Data Security
Tort Liability
Other Considerations
• Location-Based Services Defined
  – Location-Based Services refers to a broad range of services that are based on (or enhanced by) information about the physical location of a user and/or device.
  – Typical location-based services for consumers might include real-time turn-by-turn directions, the location of the nearest gas station or motel, or social networking services.

• Predictive Analytics Defined
  – Predictive analytics encompasses a variety of techniques from statistics, modeling, machine learning, and data mining that analyze current and historical facts to make predictions about future, or otherwise unknown, events.
  – In business, predictive models exploit patterns found in historical and transactional data to identify risks and opportunities.
  – Models capture relationships among many factors to allow assessment of risk or potential associated with a particular set of conditions, guiding decision making for candidate transactions.
“It’s tough to make predictions, especially about the future.”

Yogi Berra(?)
Samuel Goldwyn(?)
Niels Bohr(?)

Increasingly Omnipresent

Changes in smartphone ownership, 2011–2013
% of all U.S. adults who own...

Source: Pew Research Center’s Internet & American Life Project April 26-May 22, 2011, January 20-February 19, 2012, and April 17-May 19, 2013 tracking surveys. For 2013 data, n=2,252 adults and survey includes 1,127 cell phone interviews. All surveys include Spanish-language interviews.

Location Data Collection

What location data can be collected?

• Current location
  – GPS
  – Cell tower location
  – Wi-Fi locations
• Compass heading
The Tell-All Telephone

Striking illustration of data collected:

http://www.zeit.de/datenschutz/malte-spitz-data-retention/
LBS and Predictive Analysis

Uses of LBS Data with Predictive Analytics:

• Targeted Advertising / Marketing
• Social media
• Navigation
• Insurance / Fraud Prevention
• Law enforcement and intelligence
Predictive Analytics Can Be “Creepy”

“While it is not a universal reaction, predictive analytics in certain contexts can prompt a ‘creepy’ or unsettling feeling of being under the gaze of an omniscient observer who knows something about us and our behavior.”

http://www.priv.gc.ca/information/research-recherche/2012/pa_201208_e.asp
Emerging 3-Tier Systems in the US

• Federal
• State
• Self-Regulatory Organizations

No comprehensive regime at any level. . .
Privacy
Privacy – Federal

Federal Privacy Laws

Privacy of Communications
- The Electronic Communications Privacy Act (1986) [full text]
- Telephone Consumer Protection Act of 1991 [full text]

Children's Privacy
- Children's Online Privacy Protection Act (COPPA) of 1998 [full text]

Privacy of Financial Information
- Fair Credit Reporting Act (1970) [full text]
- Right to Financial Privacy Act (1978) [excerpts] [full text]
- Taxpayer Browsing Protection Act (1997) [full text]
- Gramm-Leach-Bliley Act (1999) [outline]
- Fair and Accurate Credit Transactions Act (2003) [full text]

Privacy of Medical Records
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) [full text]

Privacy of Miscellaneous Records and Activities
- Administrative Procedure Act [full text]
- Family Education Rights and Privacy Act (1974) [excerpts]
- Privacy Protection Act of 1980 [excerpts]
- Cable Communications Policy Act of 1984 [excerpts]
- Video Privacy Protection Act of 1988 [excerpts]
- Employee Polygraph Protection Act of 1988 [full text]
- Driver's Privacy Protection Act of 1994 [excerpts]
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 [full text]
- Do-Not-Call Implementation Act of 2003 [full text]

+ a lot more

Source: https://www.cdt.org/privacy/guide/protect/laws.php
Privacy – FTC

**Federal Trade Commission Act**

(15 U.S.C. 41, et seq)

Section 5: “Unfair or deceptive acts or practices”
Trend toward increasing enforcement

• More than 60 actions to date
• Well over half in the past 5 years
• Many more investigated but not brought
• Covering largely electronically stored data and information
• Recent trend toward privacy, but target security as well
• Increasing scrutiny of mobile data privacy
• Emphasis on “sensitive information”
“Sensitive Information”

Medical Information
Social Security Numbers
Financial Records
Precise Geolocation Data
“Sensitive Information”
“Personally Identifiable Information”
“Personally Identifiable Information”

“Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license number or other government-issued identification number; (g) prescription information, such as medication and dosage, and prescribing physician name, address, and telephone number, health insurer name, insurance account number, or insurance policy number; (h) a bank account, debit card, or credit card account number; (i) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; (j) a biometric record; or (k) any information that is combined with any of (a) through (j) above.

*In the Matter of UPromise, Inc. (FTC File No. 102 3116, Jan. 5, 2012)*
“Personally Identifiable Information”

**SCOPE**

**Final Scope:** The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties.
In re Goldenshores Technologies, LLC  
(December 5, 2013)
In re Goldenshores Technologies, LLC (2013)

• Goldenshores made a popular free app called “Brightest Flashlight Free”
• FTC asserted deception regarding the collection and sharing of information
  – Precise geolocation information
  – Unique device identifier
• Privacy Policy
  – Provided for the collection and use of certain information by Goldenshores
  – Information actually shared with advertisers and other third parties
• “Opt-out” mechanism
  – Purported to offer users an opt-out from sharing
  – Did not actually lead to an opt-out
• Notice and Consent
  – Users presented with the opportunity to accept/reject a EULA
  – Data collection and sharing began before consent was actually given
In re Goldenshores Technologies, LLC (2013)

- Case ended in settlement
- Goldenshores is prohibited from continuing misrepresentations regarding collection, sharing, and use of user information
- Goldenshores required to provide a just-in-time disclosure informing users when, how, and why their precise geolocation information is being collected, used, and shared
- Requires Goldenshores to obtain affirmative express consent before collecting, using, or sharing precise geolocation information of users

http://www.ftc.gov/sites/default/files/documents/cases/131205goldenshoresorder.pdf
• State consumer protection statutes
  – All 50 states
  – Prohibitions on “unfair or deceptive” trade practices

• 28 States have “Little FTC Acts”

• Data breach notification statutes
  – At least 46 states (DC and various US territories)
  – Notification of state residents (and perhaps regulators) affected by unauthorized access to sensitive personal information

• Data safeguards statutes
  – (Significant) minority of states
  – Safeguards to secure consumer information from unauthorized access

• Data privacy statutes
  – Online privacy policies covering use and sharing of consumer information
  – Use of personal information for direct marketing purposes
California has by far been the most active

*Privacy on the Go: Recommendations for the Mobile EcoSystem*

Recommendations for App Developers:

– Be Transparent
– Limit Data Collection
– Limit Data Retention
– Give Users Access
– Use Security Safeguards
– Be accountable

* http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf
Privacy – Industry Self-Regulation

“Consumer Privacy Bill of Rights”
Consumer Privacy Bill of Rights

• Combined effort of the White House, Department of Commerce, and the FTC
• Provides a framework for consumer privacy protections
• Establishes principles covering personal data
• Modeled off principles adopted by organizations in Europe and Asia
• Proposes voluntary industry “codes of conduct” for data privacy and security
Consumer Privacy Bill of Rights

- Industry codes of conduct
  - Voluntary privacy and security “codes of conduct”
  - Commerce Department National Telecommunications and Information Administration (NTIA) to facilitate creation
  - Other federal agencies may also convene industry stakeholders
  - Industries can also convene stakeholders absent NTIA

- Inclusive and transparent “multi-stakeholder” processes

- Enforcement authority
  - FTC to enforce codes of conduct
  - Violations constitute a deceptive practice under Section 5 of the FTC Act
  - Adherence to codes to be looked upon “favorably” in FTC investigations
NTIA

- Initial focus: Mobile devices
- Process completed: July 25, 2013
- Code of conduct released
  - Focuses on short form notices
  - “[P]rovide consumers enhanced transparency about the data collection and sharing practices of apps that consumers use.”
- Key points
  - Data collected
  - Means of accessing long-form policy
  - Data sharing
  - Identity of entity providing the app
- Next up: Facial recognition technology
Digital Advertising Alliance (DAA)

• Application of the DAA Self-Regulatory Principles to the Mobile Environment (aka the “Mobile Guidance”)
• Establishes how the existing DAA principles apply to mobile
• Keys on “Transparency” and “control” (i.e., notice and choice)
  – Transparency
    • Clear, meaningful and prominent notice of transfers (1st parties)
    • Clear, meaningful and prominent notice of collection and use practices (3rd parties)
    • Enhanced notice in certain instances
  – Consumer Control
    • Consent (1st and 3rd party)

Network Advertising Initiative (NAI)

- Mobile Application Code
- Best practices for “mobile-specific data”
  - Precise location information
  - Personal directory data
- Keys points:
  - Education
  - Transparency and Notice
  - User Control
  - Use Limitations
  - Transfer Restrictions
  - Data Access, Quality, Security and Retention

Examples

Privacy Policy Link in App Store

Opt-in
Examples

Privacy Policy Link in App

Opt-Out
Tort Liability

- *In re Apple Inc. iPhone/iPad Application Consumer Privacy Litigation*, 11-md-02250, U.S. District Court, Northern District of California (San Jose)
- Similar case involving Google: *In re Google Android Consumer Privacy Litigation*, U.S. District Court, Northern District of California
- *Rosenberg v. Harwood*, No. 100916536 (Utah District Court; May 27, 2011) (asserted Google provided bad walking directions)
Additional Considerations

- Legal process
- Law enforcement / National security
- Others
Thank you.

Bruce Antley  
Assistant General Counsel, AOL Inc.  
bruce.antley@teamaol.com

Jason Haislmaier  
Partner, Bryan Cave LLP  
jason.haislmaier@bryancave.com