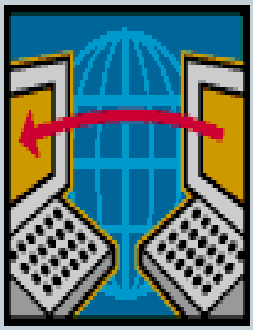
PRIVACY IN THE AGE OF ELECTRONIC COMMUNICATION

PART I

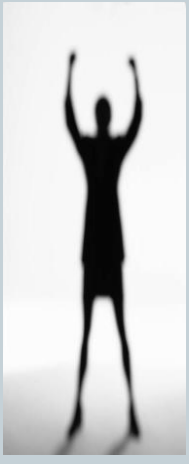
INFORMATIONAL PRIVACY



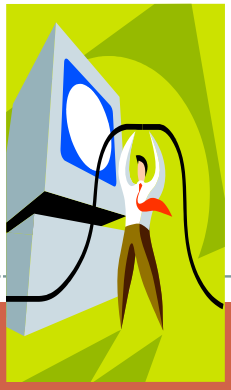
By Victoria Brown, Esq.,
342 Grand Ave,
Englewood, NJ 07631
201 567 6144
email: vb@brownllc.com

Personally Identifiable Information

- "PII", personally identifiable information, "names, addresses, telephone numbers, email addresses, dates of birth, genders, insurance statuses, education levels, occupations, medical conditions, medications…". See *In re Pharmatrak*, 329 F.3d 9 (1st Cir, 2003) at p. 15.



TRACKING



COOKIES

- Cookies are small computer programs that are typically put on an Internet user's computer by a website when that user surfs the Internet. The cookie is placed on the hard drive of a user's computer and sends back information to the entity that placed the cookie. (initially tracking only IP address and other cookies)

WEB BUGS

- Programs downloaded on a user's computer that can scan all information - documents and emails and send PII back. It has its own authorized certificates that cannot be fully uninstalled

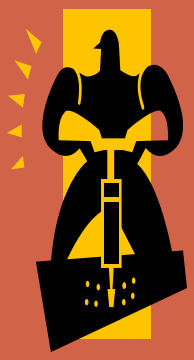
GPS TRACKING - by phones, GPS devices and beepers.

WHAT'S AN IP ADDRESS? E.g.. 123.45.67 .89

Every computer has an ***"IP address"*** (Internet protocol address) which is a form of a unique multi-digit number assigned by the user's Internet Service Provider ("ISP")..... To interact with other computers also attached to the Internet. An IP address is a string of up to twelve numbers separated by dots — for example, 123.45.67.89. Ibid.

In certain situations, a computer is assigned a permanent IP address, called a static IP address. Ibid. Most often, when an individual connects to the Internet, his or her Internet Service Provider [194 N.J. 391] dynamically assigns an IP address to the computer, which can change every time the user accesses the Internet.." [945 A.2d 29] See State v. Reid, 194 N.J. 386, 945 A.2d 26 (N.J., 2008)

DATA MINING



a/k/a

DATA

HARVESTING

- multi-billion dollar industry

COMPILING & PROFILING

- *Mike Harris and Jeff Dunstan, individually and on behalf of a class of similarly situated individuals v. comScore, Inc*, case No 11-cv-5807, U.S District for the Northern District of Illinois, 2011)

PMOS smartphone operating system from the company PEEPL

PUT ON SMARTPHONES OF MAJOR CELL PHONE PROVIDERS AND CANNOT BE UNINSTALLED, IT DOES THE FOLLOWING:

a. PMOS SOFTWARE EXPLOITED BY AD AGENCY TO DOWNLOADS USERS' VIDEOS AND PHOTOS

b. NEARME APP KNOWS THE COORDINATES OF THE USERS LOCATION AND THE PERSON THEY ARE TALKING TO

c. ROUTINELY COLLECTS SMARTPHONE USERS SERIAL NUMBERS, GPS COORDINATES, PROFILE NAME AND PHOTO AND A 3RD PARTY AD NETWORK CAN COLLECT THE SAME INFO ABOUT A USERS CHAT PARTNER

TYPES OF ELECTRONIC SURVEILLANCE

***COMMERCIAL SURVEILLANCE**

***GOVERNMENTAL SURVEILLANCE**

***CRIMINAL SURVEILLANCE**

INDUSTRY SELF-REGULATION

SEALS OF APPROVAL

like *eTrust* are no guarantee your information is kept private –

* no private cause of action
* little oversight

NO GUARANTEE OF PRIVACY

NO TRANSPARENCY

THE ETRUST "CERTIFICATION IS SO LIMITED THAT THE MAJOR SCANDALS THAT HAVE INVOLVED MICROSOFT AND INTEL WERE BEYOND ITS SCOPE.

"…..P3P DOES NOT ASSURE THAT EVEN IF IT IS HAS HIGH PRIVACY DEFAULT SETTINGS, THAT WEBSITES COMPLY WITH THESE STANDARDS. IT HAS NO MEANS TO VERIFY COMPLIANCE. … WHAT IS GOING ON CANNOT BE SEEN BY THE USER AND THUS THEY ARE UNAWARE THAT OF THE INVASION OF PRIVACY AS IT IS TAKING PLACE." *PROFESSOR JOEL R. REIDENBERG ALSO REPORTED TO CONGRESS*

Google *merges* with DoubleClick

- DoubleClick – largest display advertiser. Huge internet harvester
- Google – sells advertising space (and tracks all websites visited by an IP address).

Merger: **1 + 1 = 20**

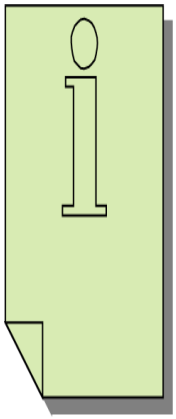
- MERGED in 2007- consumer data not yet recognized as a relevant "product market" and therefore the merger was not classified as "anti-competitive"
- 80% of all searches are done on Google

FTC AS REGULATOR

The Federal Trade Commission ("FTC") prosecutes the most egregious cases, in an attempt to protect ordinary citizens from "deceptive and unfair trade practices" on or off the Internet.

- PRIVACY POLICY FORMS

The FTC website has a privacy policy suggested form - FTC website Section 313.2 "Model privacy form and examples" and appendix A to Part 313 the model privacy form at: *www.ftc.gov*



FTC Enforcement of Privacy on the Internet

Unfair and deceptive practices"

(Section 5(a) of the FTC Act, 15 U.S.C. §45(a))

- Most cases settle – lack of resources
- Settlements with Facebook, Microsoft and many other major players –
- FTC likes to obtain 20 years oversight and audit rights

Websites are not obligated to post a privacy policy, but if one is not posted then there is a presumption of no consent to the taking of any PII

FINANCIAL STATUTORY PROTECTIONS

GLBA – FINANCIAL INFO

- Financial Information - Gramm-Leach Bliley Act of 1999 - -Title V of this Act, 15 U.S. C. §§6801-6808, subtitle A, “Disclosure of Nonpublic Personal Information”, protects a consumer from disclosure of their private financial information and requires that special safeguards be in place to protect digital and internet accessed financial data.

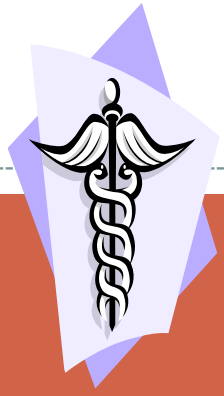
GLBA REQUIREMENTS:

- NOTICE of
- information on what data is collected (issue of transparency}
- how the data is collected and used,
- who the data is shared with and what safeguards are employed to protect the data.
- Any affiliates that are given information from the consumer must also maintain the confidentiality of the information
- Consumers must be given reasonable access to the information collected to review it and correct any errors.
- Ability to opt out

Other Financial Protection Statutes

- **RFPA – Right to Financial Privacy Act of 1978** – (12 U.S.C. §3401-3402) in response to *United States v Miller*, 425 U.S. 435 (1976) , was enacted to give one privacy to their bank records. Notice and opportunity to object to disclosure requested by subpoena (Exceptions: IRS has its own pertinent rules and Patriot Act §358 permits disclosure to an intelligence agency in an investigation related to terrorism). Issue of disclosure (delayed and if ever) of criminal investigation government requests.
- **Bank Secrecy Act – (12 U.S.C. 3413 in immunity to banks for certain reporting**
- **SAR – Suspicious Activity Report** made by banks under the RFPA §3403(c) – transactions over $25,000
- Form 8300 – 31 U.S.C. §5322 **– anyone in trade or business** must report CASH transactions over $10,000 (e.g.. sale of jewelry)
- **Federal Privacy Act (5 U.S.C. § 552a),** protects personal information gathered by U.S. government agencies
- **FCRA** – Fair Credit Reporting Act
- **FACTA** – Fair and Accurate Credit Transactions
- **EFTA** -Electronic Funds Transfer Act.

MEDICAL STATUTORY PROTECTION



HIPPA - Health Insurance Portability and Accountability Act of 1996-42 USC 1320 et seq

Practice Tip:

In discovery an attorney should use reasonable efforts to limit PHI to the "minimum necessary" to accomplish the intended purpose of the use, disclosure or request. 45 C.F.R. § 164.508.

- The background of this Act and its purpose is well explained in *Smith v American Home Prod. Corp*, 855 A2d 608, 372 N.J. Super 105 (NJ Super CH 2003)

i) Children's Online Privacy Protection Act (COPPA) -

15 U.S.C. §6501 et seq. (mirrored by §1301 et. seq) which was followed by Federal Trade Commission regulations (as authorized by the Act, 15 USC §6502) followed by implementation with 16 C.F.R. Part 312, seeks to protect children, age **thirteen and under**, from privacy data collection abuses on the Internet.

- COPPA is enforced by the Federal Trade Commission

Operators

i) must provide parents access to review and/or delete personal information provided by their children,

ii) may not condition a child's participation on the website on the child's divulging personal information

iii) must secure all information obtained from children and must keep it confidential

iv) use reasonable efforts to contact parents of information collected from children.

REGARDING CHILDREN: OPERATORS SHOULD POST THIS NOTICE ON THEIR WEBSITE

NOTICE: Visit www.OnGuardOnline.gov for tips from the Federal Trade Commission on protecting kids' privacy online

must contain a hyperlink to http://www.onguardonline.gov/topics/kids-privacy.aspx

See *United States v. W3 Innovations*, LLC (N.D. Cal., 2011)

PROPOSED LEGISLATION

The "Internet Users Bill of Rights"

- February 2012 Obama supported bill along with a proposed Do Not Track agreement
- restriction on data collection would apply to third parties (Google 40 billion in revenue would not be affected)
- Akin to the GLBA in many ways e.g.. user would have the ability to control what data is collected, and if data is collected, and a user should be able to set restrictions on its use. The bill would apply to "personal data" linked to a specific individual
- Not enforceable by individuals (FTC, State Attorney Generals)

COURT REVIEW OF Commercial PII CASES

In re Double Click, Inc, Privacy Litigation, 154 F.Supp2d 497 (S.D.N.Y. 2001) holding that tracking was acceptable and not an invasion of privacy – ONLY "IP ADDRESSES" TAKEN

In re Pharmatrak, 329 F.3d 9 (1st Cir, 2003), the court noted that more than IP addresses were taken, personally identifiable information was taken WITHOUT CONSENT . This was wrongful

ISSUES: WHAT WAS TAKEN AND WAS THERE CONSENT?

CONSENT TO PII

PRACTICE TIP: Attorney's with websites should know and understand the policies of their internet service provider and web host to find out if they are tracking more than IP addresses of users who visit their website (and include pertinent info in their privacy policy)

Privacy Policy

Must be **clear and conspicuous**

1. Clicking "I accept" best method

2. Posting policy on the website

a. is the policy on the first screen opened?

b. is there [illegible] rolling down?

c. typeset large enough?

d. easily understandable?

e. who is the info shared with?

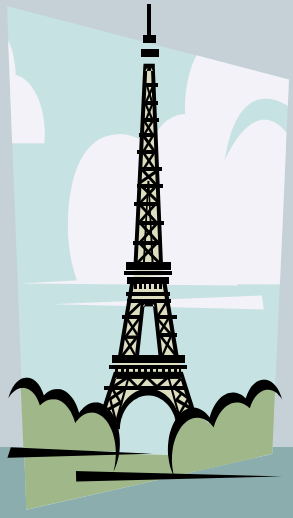
. EU Directive

- Since the 1990's, the European Union (EU) does not permit tracking of internet use of ordinary citizens or profiling based thereon. A citizen of the European Union has their Internet privacy rights guarded as a fundamental constitutional right. The European Commission's Directive on Data Privacy went into effect October 1998

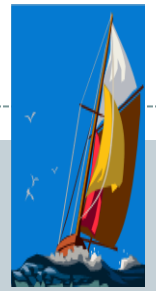
EU Privacy Requirements

For one's privacy to be compromised a European Union citizen must

- a) consent to his/her data collection,
- b) be informed as to exactly how their data will be used,
- c) have access to the data to make corrections and
- d)have the collectors of the data appropriately secure it.



EU Treaty with the US Safe Harbor Provisions



If a company is not registered with Safe Harbor, there is a “presumption” that the data will not be adequately protected.

There is a list of US companies that have self-certified and are listed as compliant with the European Directive above mentioned
See the US Dept of Commerce website at

www.export.gov/safeharbor

New Jersey privacy rights highly guarded

- *State vs Reid*, [194 N.J. 386 at 397-398, 945 A.2d 26(N.J., 2008)

residents have a right to privacy in their telephone use and bank records (State vs Reid, [194 N.J. at 397-398] and thus should likewise have a right of privacy in their Internet Service Provider (ISP) records. Personal data given to an internet service provides has certain protections and requires a subpoena.

The New Jersey Supreme Court in State v. Reid, 194 N.J. 386, refused to accept the State's argument that IP addresses were the same as return addresses on an envelope because the later were voluntarily put on the envelope and were known to be viewed by others.

> *The NJ Supreme Court refused to endorse PII rights any further in this case except as to ISP records. It would not yet agree to extend its definition of PII, as proposed by the Appellate Division*

ATTORNEY PRACTICE

- Rule 1:38 – when an attorney files a statement, any personal identifiers have been redacted. Rule 5.2 of the Federal Rules of Civil Procedure entitled "Privacy Protection for Filing Made with the Court" requires redaction of personal identifiers (which includes names of minors (to be identified by initials),

- Personal Identifiers are defined as social security number, driver's license number, vehicle plat number, insurance policy number, active financial account number or active credit card number. However, the last four digits of an active financial account need not be redacted if the account is the subject of the litigation and cannot be otherwise identified.

- The updated Case Information Statement that is filed with a Superior Court civil case action has the appropriate language in the form at the bottom that states, "I certify that confidential personal identifiers have been redacted from documents now submitted to the court, and will be redacted from all documents submitted in the future in accordance with Rule 1:38-7(b)". This should be added to Special Civil Part complaints.

NOTHING ON THE INTERNET IS PRIVATE

- New York Times, 2/28/2012 reported that applications downloaded on Apple devices were taking peoples addresses and photos and that Apple has 600,000 “apps” and cannot vigilantly monitor them all.

- Cloud computing – dubious protections

GOVERNMENTAL SURVEILLANCE

- Foreign Intelligence Surveillance Act ("FISA")50 USC §§1801 et seq.

- *Jewel et. Al vs. National Security Agency et. al*, US Court of Appeals, Ninth Circuit, 21605, Dec. 29, 2011, the plaintiffs sued American security agencies for "what they describe as a communications dragnet of ordinary American citizens." The plaintiff was a subscriber to AT&T telephone and internet services and claimed:

"[u]sing [a] shadow network of surveillance of devices, Defendants have acquired and continue to acquire the content of a significant portion of phone calls, emails, instant messages, text messages, web communications and other communications, both international and domestic, of practically every American who uses the phone system or the Internet, including Plaintiff and class members, in an unprecedented suspicionless general search through the nation's communications network".

Foreign Intelligence Surveillance Act ("FISA")50 USC §§1801 et seq.

- of 1978 ("FISA" Pub.L. 95-511, 92 Stat. 1783, enacted October 25, 1978, 50 U.S.C. ch.36, S. 1566)
- electronic surveillance and collection of "foreign intelligence information" between "foreign powers" and "agents of foreign powers" (which may include American suspected of being engaged in espionage).

- District Court: Plaintiffs denied as lacking "heightened standing" to sue government officials in a national security context

- Circuit Court: "Injury in fact" gave standing – private cause of action under FISA

Also see *Amnesty Int'l United States v Clapper*, 638 F3d 118, 122 (2nd Cir 2011)

Patriot Act

- Modified FISA
- See American Civil Lib Union v US Dept. of Justice, 265 F. Supp2d 20 (D.D.C, 2003)
  - A. test – activity or record concerns an authorized investigation to protect against terrorism
  - B. no warrant required for pen register/telephone, email, or looking for and taking tangible things (e.g. documents)
  - C. "sneak and peak" –"covert entry to seize intangibles", no notice required if officer thinks it will have an adverse result

* Telephone company immunity (see Jewel et. Al vs. National Security Agency et. Al, US Court of Appeals, Ninth Circuit, 21605, Dec. 29, 2011)

CRIMINAL SURVEILLANCE

"Phishing" is using a fake email or website to collect data and/or get money ..

"Pretexting" pretending to be someone you are not – impersonating a real internet user.

"Hacking" – In June 2012 Linked In was hacked and passwords of 6 million users stolen.