Privacy Rules and the Internet:

When (If Ever) Can You Search a Party's Computer?

Presented to
Civil Practice Update:
Review on E-Discovery
Illinois State Bar Association
May 19, 2016

by

Michael D. Gifford
Howard & Howard Attorneys PLLC
One Technology Plaza
211 Fulton Street, Suite 600
Peoria, IL 61602-1350
309-672-1483
mgifford@howardandhoward.com

I. Introduction

Data privacy rules are one of the most vexing issues facing business today. Review of Electronically Stored Information ("ESI") is often seen as a different problem than procedures to address data privacy requirements. For eDiscovery purposes, it is no longer enough (if it was ever) to simply catalog each custodian's data sources (*i.e.,* hard drives, network shares, e-mail, flash drives, CDs/DVDs, smartphones, and often home or personal computers and devices) and system sources (*i.e.,* databases or subject matter folders not "owned" by a specific custodian), and collect the identified data for processing. Depending on the nature of the data, the custodian's position, and relationship to the party responding to e-discovery, it may also be necessary to consider privacy rights regarding data stored on the party's systems. Those privacy rights may belong to a custodian, a customer or applicant, or a third-party.

The presentation will review some of those data privacy rights, both in the United States and abroad.

This presentation will also address issues which can arise if a party seeks to compel production of an opposing party's devices for examination.

II. Systems Awash In Private Data

Many data systems contain data subject to one or more confidentiality requirement. Many systems intentionally collect and store confidential data regarding employees, applicants, customers, and business partners, including personal information such as dates of birth, and social security numbers, banking and credit card data, health records, employment records.

In addition to the confidential data systems may intentionally contain, confidential data requiring protection may creep unintentionally into a system. Virtually any entity which has two or more computers, or two or more custodians, will have at least an informal policy which says, in effect, "nothing you do on this computer is private, we have the right to review everything, with or without notice." Despite the multitude of policies which say "e-mail and the use of this computer system is for business only" virtually every company allows at least some, reasonable use of their systems for personal e-mails (i.e., Honey-Do and "who's picking up the kids" communications) and networks for personal browsing. Such e-mails and browsing histories may be awash in confidential data about employees and their families, including financial, medical, educational, and purchasing histories.

Data may be subject to statutory or regulatory protection, or it may also be subject to contractual protection. Data shared subject to a confidentiality or non-disclosure agreement, while lacking statutory protection, is subject to contractual protection, the breach of which can create expensive and embarrassing liability.

The amount of data stored is staggering. Although not directly related to eDiscovery, a cyber crime statistic helps highlight the problem. It is estimated that last year's Target data

breach alone resulted in disclosure of 40 million records with credit and debit card records of Target shoppers. More than 70 million records with names, addresses, email addresses and phone numbers were exposed.

III. Data Privacy Rules

As litigators, we're all aware of the obligation to protect and not file confidential data such as social security numbers. Amendments to the Federal Appellate, Bankruptcy, Civil, and Criminal Rules of Procedure address issues relating to privacy and public access to electronic case files. The Rules require that filers redact certain "personal identifier" information, such as Social Security or taxpayer-identification numbers, dates of birth, names of minor children, financial account numbers, and in criminal cases, home addresses, from their filings.[1] Despite these long standing rules, redaction errors continue.[2] Embarrassingly, even courts have problems: a recent "redacted" decision issued by the U.S. District Court for the Western District of Washington was readily readable due to faulty redaction technique.[3] Many states have similar filing requirements.

In addition to court rules, several federal statutes impose privacy and non-disclosure obligations. Those statutes include:

Gramm-Leach-Bliley Act ("GLBA"): GLBA protects a customer's personal information held by financial institutions. "Financial Institution" is broadly defined, and includes "all businesses, regardless of size, that are "significantly engaged" in providing financial products or services." The definition includes non-bank mortgage lenders, loan brokers, some financial or investment advisers, tax preparers, providers of real estate settlement services, and debt collectors, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, courier services, credit reporting agencies and ATM operators that receive information about the customers of other financial institutions.[4]

---

1 Fed. R. App. P. 25(a)(5); Fed. R. Civ. P. 5.2; Fed. R. Crim. P. 49.1; Fed.R. Bankr. P. 9037.

2 Frangiosa, Christina D, *Redaction Failures Continue in Electronic Court Filings, Study Shows* , Privacy and IP Law Blog, 2/10/16, http://privacyandip.blogspot.com/2011/06/redaction-failures-continue-in.html

3 Cushing, Tim, *Redaction Failure In FTC/Amazon Decision Inadvertently Allows Public To See Stuff It Should Have Been Able To See Anyway*, techdirt, 4/29/16, https://www.techdirt.com/articles/20160428/09572134302/redaction-failure-ftc-amazon-decision-inadvertently-allows-public-to-see-stuff-it-should-have-been-able-to-see-anyway.shtml; Davis, Wendy, *Judge: Amazon Bilked Parents For Kids' In-App Payments, Ruling Disclosed By Digital Glitch*, The Daily Online Examiner, 4/27/16, http://www.mediapost.com/publications/article/274457/amazon-wrongly-charged-parents-for-kids-in-app-pu.html

4 Federal Trade Commission, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, April 2006, https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying; Federal Trade Commission, *In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act,* July 2002, https://www.ftc.gov/tips-advice/business-center/guidance/ brief-financial-privacy-requirements-gramm-leach-bliley-act;

GLBA requires notice to customers prior to disclosure, and entry of an appropriate protective order protecting a customer's private information.[5]

Right to Finance Privacy Act ("RFPA"): The RFPA is somewhat similar to, but more limited than the more recent and comprehensive GLBA. The RFPA protects against disclosure of the financial records of certain customers (individuals and partnerships of five or less persons) to the federal government or its agencies. It does not govern disclosures to private entities or state or local governmental bodies, although Illinois[6] and several other states have comparable laws. The law, in effect, creates a statutory Fourth Amendment right for certain parties related to financial records..

Health Insurance Portability and Accountability Act ("HIPAA"): HIPAA restricts disclosure of personally identifiable health information by most health care providers. HIPAA preempts state law, unless the state law provides more stringent protections. Disclosure may be made where the subject of the data provides an authorization, or where disclosure is ordered by a Court. Disclosure is also authorized pursuant to a discovery request (as distinguished from an order of the court) where the health care provider is provided with "satisfactory assurance" that the information will remain confidential. Satisfactory assurances essentially means a qualified protective order.[7] A qualified protective order means one that prohibits use of the protected health information for any purpose other than the litigation and requires return or destruction of the data after the litigation ends.[8]

Disclosures must always be restricted to the minimum necessary information in the context of the disclosure.[9]

Health Insurance Technology for Economic & Clinical Health Act ("HITECH"): HITECH amended HIPAA to impose most of its obligations on HIPAA Business Associates as well as health care providers. Vendors and services providers to "covered entities," including law firms are now directly subject to HIPAA's privacy requirements, and must comply with HIPAA in collection and

---

5 *Marks v. Global Mortgage Group, Inc.*, 218 F.R.D. 492 (S.D.W.Va.2003); *Powell v. Huntington Nat'l Bank*, CASE NO. 2:13-cv-32179 (S.D.W. Va. Oct 30, 2014)

6 The Illinois statute is broader than its federal counterpart:
(c) Except as otherwise provided by this Act, a bank may not disclose to any person, except to the customer or his duly authorized agent, any financial records or financial information obtained from financial records relating to that customer of that bank unless:
(1) the customer has authorized disclosure to the person;
(2) the financial records are disclosed in response to a lawful subpoena, summons, warrant, citation to discover assets, or court order which meets the requirements of subsection (d) of this
(3) the bank is attempting to collect an obligation owed to the bank and the bank complies with the provisions of Section 2I of the Consumer Fraud and Deceptive Business Practices Act. 205 ILCS 5/48.1(c)
A similar provision pertains to credit unions: 205 ILCS 305/10.

7 45 CFR §164.512(e)

8 *Id.*

9 45 CFR 164.502(b), 164.514(d)

processing ESI. The amendments also expand the universe of Business Associates, reaching down stream to include sub-contractors providing services for covered entities under a Business Associate (*i.e.*, investigators, e-discovery vendors, etc.)[10]

Children's Online Privacy Protection Act ("COPPA"): COPPA[11] protects the privacy of children under the age of 13 by requesting parental consent for the collection or use of any personal information of the users. Beyond establishing safeguards on the collection and retention of information regarding child users, COPPA requires that website operators protect the confidentiality, security, and integrity of any personal information that is collected online from children. COPAA defines personal information to include names, addresses, e-mail addresses, social security numbers and any personally identifiable information regarding a child or his/her parent, such as IP addresses or customer IDs.[12]

Beyond federal statutes, certain state statutes impose transfer and/or notification requirements. For example, the Illinois Banking Act requires notification to bank customers when their data is disclosed in the course of litigation. [13]

Further complications arise when considering disclosure of data held in other countries, particularly within the European Union ("EU"). Prior to the fall of 2015, pursuant to a Safe Harbor provision negotiated under the European Commission's Data Protection Directive, U.S. companies were allowed to self-certify their compliance with EU transfer restrictions on personal data. That agreement was invalidated by the EU Court of Justice in October 2015.[14] The framework of a new agreement was announced in February, 2016, but the future viability of the new agreement is uncertain.[15]

---

10 Brown, Brian and Tijerina, Danny, *2013 HIPAA/HITECH Amendments: How the Changes Impact the eDiscovery Process*, The Health Lawyer, Vol. 27, No. 4, April 2015, http://renewdata.com/wp-content/uploads/2015/05/The-Health-Lawyer-April-2015-2013-HIPAA-HITECH-Amendments-How-the-Changes-Impact-the-eDisc-Process.pdf.

11 15 USC 6501. The Federal Trade Commissions COPPA rule is found at 16 CFR Part 312.

12 15 USC 6501(8)

13 205 ILCS 5/48.1

14 *European Court of Justice Invalidates U.S.-EU Safe Harbor Agreement*, Barnes & Thornburg Legal Alert, Data Security and Privacy and EDiscovery, Data & Document Management Law, October 2015, http://www.btlaw .com/data-security-and-privacy-and-ediscovery-data--document-management-law-alert---european-court-of-justice-invalidates-us-eu-safe-harbor-agreement-10-09-2015/; *US-EU Safe Harbor Invalidated: What Now?,* The National Law Review, October 7, 2015, http://www.natlawreview.com/ article/us-eu-safe-harbor-invalidated-what-now.

15 Nagel, Jeffrey L., *New "Privacy Shield" Agreement Seeks to Resurrect a Safe Harbor for EU-U.S. Data Transfers – Can it Succeed?,* Gibbons E-Discovery Law Alert, February 4, 2016, http://www.ediscoverylawalert.com/2016/02/articles/legal-decisions-court-rules/new-privacy-shield-agreement-seeks-to-resurrect-a-safe-harbor-for-eu-u-s-data-transfers-can-it-succeed/; Scott, Mark, *U.S. and Europe in 'Safe Harbor' Data Deal, but Legal Fight May Await*, The New York Times, February 2, 2016, http://www.nytimes.com/2016/02/03/technology/us-europe-safe-harbor-data-deal.html?_r=0

IV. Security over received data

Privacy provisions can extend the duty to protect confidential information beyond those who "own" or disclose the information. For example, the HITECH amendments to HIPAA extended that duty to Business Associates and sub-contractors. HIPAA can create liability for lawyers who represent covered entities and come into possession of personal health information.[16] Moreover, an appropriately drafted protective order will include restrictions on republication or allowable use of confidential data. For both of these reasons, attorneys and others who come into possession of confidential data must take appropriate steps to ensure its security.

V. Best Practices

1. **Recognize the Risk.** Privacy professionals are often not involved in ESI issues. The company must address that issue, and find a seat at the planning table for those persons. They will often be better versed in recognizing the risk than will litigators. Involve them early, in the planning process, not just as firefighters.

2. **Review your Privacy Rules.** HIPAA, GLBA and others require promulgation of privacy notices, familiar to any physician's new patients or periodically stuffed with mailed credit card bills. Do your ESI data collection plans refer to or incorporate those rules?

3. **Identify Probable Locations of Private Data.** Once data to be protected is identified, the locations where that data is held should be charted.

4. **Limit Collection to What is Strictly Necessary.** Counsel, in-house included, will often default to "over-collection:"collecting everything and limiting disclosure in the filtering and review process. Narrowly tailored collection can minimize the risk.

5. **Use "Meet and Confer" to Your Advantage.** Consistent with limited collection, address these issues early with opposing counsel and seek agreements to limit collection and production. Be prepared to identify the nature of confidential data and the protection it requires. Seek agreements to eliminate entire sets of confidential data, such as social security numbers, if it is not relevant to your case. Opposing counsel often will not want confidential data which exposes them to a data breach.

6. **Review and Update Vendor Agreements and Protocols.** E-discovery vendors need to treat confidential data with appropriate security. If your agreements do not require vendors to afford enhanced security to confidential data, consider updating the Agreement. Discuss with the vendor the nature of the data, the type of security it requires, the harms, including expense,

---

16 *New HIPAA Liability for Lawyers*, GPSOLO, Vol. 30, No. 4, American Bar Assn, http://www. americanbar. org/publications/gp_solo/2013/july_august/new_hipaa_liability_lawyers.html

which would arise from disclosure, and how to allocate the risk. If your vendor agreement does not indemnify the company and counsel for disclosures while in the vendor's control, consider requiring an amendment.[17]

VI. Other Privacy Problems

Beyond the problems discussed above, the ready availability of personal information through the Internet can raise other issues.

A. Are you REALLY Friends? Social media can be a valuable applicant vetting tool for recruiters, but it also presents risks, particularly when the subject is a current employee. Not all social media is created equal, and the information found there must be carefully weighed for accuracy.[18] Social media review can implicate EEO discrimination problems that would otherwise not exist.[19] Social media review of an applicant conducted by a third party raises Fair Credit and Reporting Act disclosure obligations.[20]

Use of social media with current employees is additionally problematic under Illinois law: the Personnel Record Review Act provides that "an employer shall not gather or keep a record of an employee's associations, political activities, publications, communications or nonemployment activities. . . " absent permission, except in narrow circumstances implicating workplace safety.[21] Any such records are personnel records, requiring disclosure to the employee on request.

B. Employee E-mail: Does Attorney-Client Privilege Exist Within the Employer's E-mail?

An e-discovery headache for employers is what to do with an employee's "private" e-mail on the employer's system, particularly e-mail intended as attorney-client privilege. Scenario: Bank lending officer leaves Bank A to work for Bank B, and Bank A files suit against employee and Bank B to seek enforcement of restrictive covenant, trade secrets, and other assorted claims. Bank B has typical e-mail policy reserving the right to examine any e-mail, and declaring that employees have "no expectation of privacy." Typical of other employers, Bank B allows

---

17 For additional discussion of best practices, see Leffert, Kim A, Dargar, Seema V., and Lackey, Michael E, *E-discovery and Data Privacy in the US*, Lexology, June 30, 2011, http://www.lexology.com/ library/ detail.aspx?g=77ddac3d-fd89-4abd-9cc8-3b33b1c26785

18 Koch, Brittany B,. *Vetting Employees via Social Media – Walking the Digital Tightrope,* April 20, 2015,The National Law Review, http://www.natlawreview.com/article/vetting-employees-social-media-walking-digital-tightrope

19 Hyman, J., *Social Media Background Checks as Discrimination*, Lexis-Nexis Legal Newsroom, Labor & Employment Law, Dec. 2, 2013, https://www.lexisnexis.com/legalnewsroom/labor-employment/b/labor-employment-top-blogs/archive/2013/12/02/social-media-background-checks-as-discrimination. aspx? Redirected=true

20 Fair, L, *The Fair Credit Reporting Act & social media: What businesses should know*, Federal Trade Commission, June 2, 2011, https://www.ftc.gov/news-events/blogs/business-blog/2011/06/fair-credit-reporting-act-social-media-what-businesses.

21 820 ILCS 40/9

reasonable personal use of its e-mail system. Employee and his counsel (not Bank B's counsel) use the employer's e-mail to communicate and those e-mails are caught in ESI collection, and after several objections, arguments, motions to compel and for sanctions, the Court orders production by Bank B to Bank A of otherwise privileged communication.

Employers involved in litigation will face this situation.[22] It becomes even more problematic where the employer and employee are opposing parties, and the employer is faced with the chance to read the employee's attorney-client communication. The current trend is that use of an employer's e-mail system where there is no expectation of privacy strips the attorney-client protection.

C. Searching an Opponent's Computers

Occasionally, a party will go beyond a simple request for discovery of documents and ESI, and seek production of computers, hard drives, or other storage media for forensic examination. Such requests are fraught with confidentiality issues, including many of those discussed above. The 2006 Advisory Committee Notes to the amendments to Federal Rule of Civil Procedure 34 stated that:

> Inspection or testing of certain types of electronically stored information or of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems.

The better rule is that such examinations should not be compelled absent a history of discovery abuse by the producing party. *Calyon v. Mizuho Securities USA, Inc.*, No. 07CIV02241RODF, 2007 WL 1468889 (S.D. N.Y. May 18, 2007).

> In sum, the Court is not yet faced with any failure by the defendants to conduct a thorough forensic search of their computers, or to produce any and all relevant documents, files, metadata, and even hidden data fragments that Calyon may request. On the contrary, the Individual Defendants have represented that their expert can and will conduct an exhaustive search of the hard drives for the information Calyon seeks, including information located in the hard drives' hidden areas . . . and the Court, at present, has no basis to question this representation. 2007 WL 1468889, at *5.

---

22 *First Financial Bank, N.A. v. Bauknecht*, 71 F.Supp.3d 819 (C.D. Ill, 2014).

More recently, it was stated that:

> The request for an inspection of the computer is denied. Such inspections by an adversary—even by a forensic expert, which movants do not suggest they have engaged—are granted only under limited circumstances, when there is reason to believe that a litigant has tampered with the computer or hidden relevant materials despite demand for them in the course of the lawsuit or when the possession or use of the computer is an element of the parties' claims or defenses. . . . This limitation reflects the fact that production of a computer to the adversary almost invariably will lead to disclosure of quantities of documents that are entirely irrelevant or privileged, and, even if not privileged, possibly quite sensitive.
>
> *Lifeng Chen v. New Trend Apparel Inc.,* No. 11 Civ. 324(GBD)(MHD), 2012 WL 4784855, *1 (S.D. N. Y. Oct. 2, 2012)

Even in cases of alleged spoliation, the better course is to require production of a forensic copy for safe keeping by a neutral or the party's counsel, or a neutral copying and examination with any data reviewed by the producing party's counsel for privilege and confidentiality prior to production.