

Finding a Needle in a Haystack:

A FORENSIC COMPUTING CASE STUDY

SUMMARY

In 2003, the U.S. Court of Appeals for the First Circuit issued a ruling clarifying how to apply the Electronic Communications Privacy Act (ECPA) to Web technology, specifically what constitutes "protected content."

In the Pharmatrak Privacy Litigation, Interhack

- described Web technology in a way that the court could understand
- collected, searched, and analyzed a tremendous amount of data under serious time constraints
- provided expert testimony that became the foundation for leading Internet privacy case law

Background

In August 2000, a lawsuit was filed against Pharmatrak, a dot-com that sold its service, *NETcompare*, to pharmaceutical companies, including Pfizer, Pharmacia, SmithKline Beecham, Glaxo Wellcome, and Novartis. Pharmaceutical companies invited consumers to visit their Web sites to learn about their drugs and obtain rebates. With *NETcompare*, these pharmaceutical clients could access information about Internet users, allowing them to do intra-industry comparisons of Web site traffic.

The Consolidated Amended Class Action Complaint alleged that Pharmatrak secretly intercepted and accessed Plaintiffs' personal information through surreptitious use of 'cookies' and other Web devices, violating the ECPA.

Pharmatrak claimed its software was not designed to collect personal information, like name, date of birth, and email address, and emphatically stated that no such personal data was collected. Pharmaceutical companies vowed they had not authorized Pharmatrak to collect such information, nor had they wanted the firm to do so.

The Defense filed a motion for summary judgment, requesting the district court to dismiss the case outright. The court allowed a very brief period for discovery, and the Plaintiffs' counsel was faced with producing evidence showing how *NETcompare* intentionally intercepted personal information and consequently violated the ECPA.

Objective

Lead attorney for the Plaintiffs, Bill Doyle of Lerach Coughlin Stoia Geller Rudman & Robbins LLP, needed a technology expert to find in Pharmatrak's server logs what the Defense claimed did not exist. Doyle found Interhack, a forensic computing company, on the Web. After reading Interhack's research paper "What's Related? Everything But Your Privacy, he knew he had found the expertise he needed. Interhack had developed a reputation for unusual mastery of computer and network technology. Subsequently, Doyle recruited Interhack's founder, Matthew Curtin, to serve as his chief forensic computer scientist.

In order for the Plaintiffs' attorney to demonstrate a privacy violation, Curtin would need to prove that personal information was not only *collected* but also *intentionally intercepted*. Pharmatrak's 80 servers contained a tremendous amount of information – the proverbial haystack.

Actions

With only days to search the Pharmatrak computers, Curtin quickly identified which of the systems contained relevant information. In less than two hours, he designed and wrote a software program that extracted the information necessary to oppose the motion for summary judgment. Interhack's role in this case was critical for several reasons:

- Interhack copied huge amounts of data, uncovering personal information of hundreds of Internet users on Pharmatrak servers.
- Curtin's custom programming very quickly and effectively uncovered the most relevant information.
- By drawing analogies to non-technical examples, Curtin helped the judge understand the implications of the technology in order to weigh the evidence.

- Curtin prepared an affidavit and produced a 1,500-page compendium of exhibits, demonstrating how Pharmatrak was collecting personal information that it affirmed to its clients and to the court that it did not.
- The Defense was unable to discredit Interhack's discovery and subsequent data analysis.

The district court entered summary judgment for the Defendants on the basis that Pharmatrak's activities fell within an exception to the ECPA statute where one participant in a communication consents to an interception. The court ignored the testimony of the pharmaceutical company executives and found that the companies had consented to the data interception by contracting with Pharmatrak. Plaintiffs found the evidence produced by Interhack sufficiently compelling to appeal.

Resolution

The U.S. Court of Appeals for the First Circuit ruled that the district court had incorrectly interpreted the 'consent' exception to the ECPA, and agreed that the content of an electronic communication was intercepted by Pharmatrak under ECPA. The circuit court ruled to reverse and remand the case because the question of the interception's legality — which depends upon specific intent — was not squarely addressed before the court.

In its ruling, the U.S. Court of Appeals for the First Circuit relied on Curtin's expert testimony to find that "content" protected under the ECPA can include part of URLs — Web addresses that include the results of fill-out forms such as search terms. This opinion now serves as leading Internet privacy case law.

"Electronic discovery is very common in litigation. Most other consultants use third-party, off-the-shelf software to analyze data. But, generic programs may not extract the data you are looking for and may introduce unexpected errors. Matt Curtin is a programmer, and he creates his own tools, rather than relying upon others' tools; this has always been a credible benefit. Because Curtin and his Interhack team work with raw data, this gives counsel an extra level of confidence that the evidence is accurate — and will hold up in court." — Bill Doyle, Partner, Lerach Coughlin

Interhack: Demystifying Computing Technology

As computing technology becomes increasingly important in the practice of law, so does the need for understanding the technology, finding electronic facts and interpreting them in the context of a specific case.

Founded in 2000 by computer and information science researchers in Columbus, Ohio, Interhack is a professional services firm with practices in both Information Assurance and Forensic Computing.

Interhack Forensic Computing serves the legal system by finding facts through collection and analysis of electronic information. Services we provide support adjudication in civil litigation as well as criminal proceedings. Demystifying technology for attorneys, judges, and juries, we use computer science to establish the facts, and provide informed, impartial opinions, allowing the legal process to follow its course.

Aside from acting as undisclosed technology consultants in numerous cases, we have served as testifying experts in cases such as Sony BMG "Rootkit" Litigation, RIAA v. MP3Board.com, Avenue A Privacy Litigation, and the Pharmatrak Privacy Litigation, which led the First Circuit to establish standards for application of Federal wiretap statutes to Web technology.

Interhack Forensic Computing Services

- **Expert Testimony** – Testimony for the court on technical matters.
- **Forensic Consultation & Analysis** – Technical analysis of data or programs for legal argumentation. Explanation of computer or networking technology to attorneys, including assistance in definition of discovery, deposition, and the cross-examination of experts.
- **Data Recovery** – Recovery and reconstruction of data, apparently deleted, damaged or lost.
- **Electronic Discovery** – The routine collection and reporting of electronic documentation in evidence.

When you have a case where technology matters, we'll be happy to talk to you about the issues at stake, how we can help, and offer strategies to answer critical technical questions without breaking the bank.

We have supported even the most high-risk and complex adjudication.

We can do the same for you.