DFRWS
DIGITAL FORENSIC RESEARCH CONFERENCE

Digital Forensics in Consumer Online Privacy Class Actions

By

Scott A. Kamber

Presented At

The Digital Forensic Research Conference

DFRWS 2011 USA New Orleans, LA (Aug 1st - 3rd)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

Digital Forensics in Consumer Online Privacy Class Actions

DFRWS 2011
New Orleans
August 1, 2011

David A. Stampley
KamberLaw
New York, Los Angeles, Healdsburg

Forensics cases: web-centric

- ***Wormley v. Geocities*** (L.A. Cty. Sup. Ct. 1999)data leakage via referer URL
- ***Lane v. Facebook*** (N.D.Cal. 2010) bug in automated notice/consent
- ***Slater v. Tagged*** (N.D. Cal. 2010) address book hijack; insecure credentials in email
- ***Valdez-Marquez v. Netflix*** (N.D.Cal. 2010) de-anonymization of large data sets

Forensics cases: web-centric (cont.)

- ***Bose v. Interclick, McDonalds …*** (S.D.N.Y. pending) browser history sniffing
- **Adobe Flash LSO cases** (C.D.Cal. 2011 & pending) “Flash cookie” circumvention of browser controls
- ***Del Vecchio v. Amazon*** (W.D.Wash. pending Flash LSOs; P3P compact policy spoofing
- ***Garvey v. Kissmetrics, Hulu*** (N.D.Cal. pending) Flash LSO + HTML5 + CSS/browser cache hack

Forensics cases: device-centric

- ***In Re ATI Tech. HDCP Litigation*** (N.D.Cal. 2009) high-def monitors
- ***In re Sony BMG CD Technologies*** (S.D.N.Y. 2006) DRM rootkit software

Forensics cases: hybrid

- **ISP DPI cases** (multiple pending)
  ISP wiretapping with DPI devices
- ***Lalo v. Apple*** (N.D.Cal. pending)
  iDevice data transfer to 3rd parties via apps
- ***King v. Google*** (N.D.Cal. pending)
  Android device data transfer to 3rd parties via apps

Application in the wild

- *When* investigation; confirmatory discovery before the environment changes
- *What* user-website traffic; user device
- *Output* preserved HTML source, scripts, traffic capture/analysis (Wireshark); user device artifacts (LSOs, cookies); defendant privacy policies, terms of use

E.g., Flash LSO, mobile device, & browser history sniffing cases

Black-box application

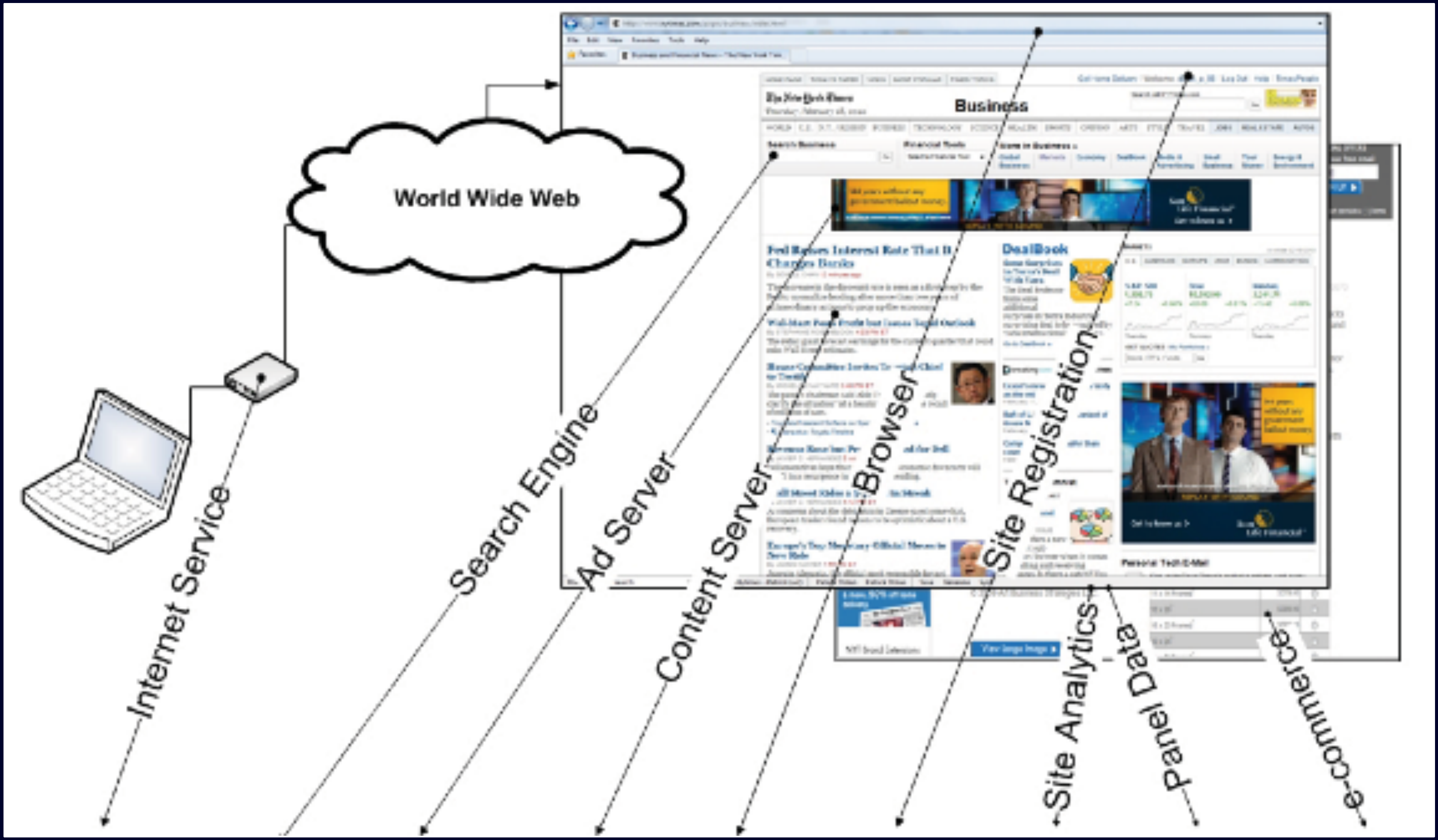
- *When* investigation; confirmatory discovery *after* environment changes
- *What* discovery materials from defendant (contracts, specs, sales materials, Congressional testimony, depositions)
- *Output* expert declaration & deposition

E.g., ISP DPI device cases

Key points

- Timing: before or early in case
- Scope: Internet-wide sampling
- Purpose: who is doing what to whom
- Outcome: resolution

Origins: online environment



World Wide Web

Internet Service

Search Engine

Ad Server

Content Server

Browser

Site Registration

Site Analytics

Panel Data

e-commerce

“Historical” influences on environment

Trends