

# PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Volume 29 Number 16 September 2, 2009

**CAPITAL INSIGHTS:** *Leading consumer and privacy groups Sept. 1<sup>st</sup> called on Congress to enact strong legislation to protect online privacy. Rather than a bill narrowly targeted at behavioral advertising, the groups urged lawmakers to enact a broad measure based upon a robust set of fair information practice principles, including limits on both collection of sensitive information and secondary use, a ban on digital redlining, and rights of access to and correction of data maintained on individuals. (For specifics on principles and groups, go to the “Newsroom” at [www.uspirg.org](http://www.uspirg.org).) Their announcement came on the eve of stepped-up, bipartisan Congressional activity. Among those cooperating on draft proposals are Reps. Henry Waxman (D-CA) and Joe Barton (R-TX), the chair and ranking member of the House Energy & Commerce Committee, and Bobby L. Rush (D-IL), chair of the panel’s Subcommittee on Commerce, and Rick Boucher (D-VA) and Cliff Stearns (R-FL), chair and ranking member of the Communications Subcommittee. The Interactive Advertising Bureau (IAB) is leading industry opposition to legislation. It unveiled a self-regulatory program earlier this year. [www.iab.net/insights\\_research/530468/iab\\_news/iab\\_news\\_article/682037](http://www.iab.net/insights_research/530468/iab_news/iab_news_article/682037)*

## MAJOR STORIES IN THIS ISSUE

**Online Ad Networks Intensify  
Capture of Personal Data . . . 1**

**SSA Pays \$500 Million After  
Computer Matching Effort . . . 6**

**FCRA: Statutory Damages  
Available w/o ‘Actuals’ . . . . 3**

**NY Times Loses Bid To Get  
Spitzer Wiretap Records . . . 6**

**Judge Dismisses Challenge To  
‘No-Fly List’ Detentions . . . 4**

**FOIA Ct. Roundup: Customs  
Vaughn; HUD Complaints . . 7**

## SOCIAL NETWORKING SITES HELP EXPOSE IDENTITY – THE MISSING LINK

Online Social Networks (OSNs) like FaceBook and MySpace are playing a key role in identifying Internet users to third-party advertisers like DoubleClick, raising the prospect of a new generation of files on the online activities of millions of individuals, researchers have found.

The significance of the findings is underscored by the fact that key House members soon are expected to unveil privacy legislation covering behavioral advertising and more. Most online

companies opposed to legislation insist that while there is tracking of computer users' online activities, such tracking is not linked to their actual identities. While that might have been truer in previous years, the new research casts serious doubt on such claims going forward.

The study, "On the Leakage of Personally Identifiable Information Via Online Social Networks," was co-authored by Balachander Krishnamurthy, a researcher at AT&T Labs, and Craig E. Wills, a computer science professor at the Worcester Polytechnic Institute in Massachusetts. It was presented in late August to the Association for Computing Machinery's Second SIGCOMM Workshop on Online Social Networks in Barcelona, Spain.

Researchers found that OSNs assign a unique identifier to their members, which is "leaked" through a combination of "HTTP header information" – the "Referer header" and the "Request-URI" – and cookies sent to third-party aggregators such as Google DoubleClick, Google Analytics, and Omniture, among others.

"We show that most users on OSNs are vulnerable to having their OSN identity information linked with tracking cookies," the authors wrote. "The two immediate consequences of such leakage: First, since tracking cookies have been gathered for several years from non-OSN sites as well, it is now possible for third-party aggregators to associate identity with those past accesses. Second, since users on OSNs will continue to visit OSN and non-OSN sites, such actions in the future are also liable to be linked with their OSN identity."

"Cookies and other tracking mechanisms on the Internet have been prevalent for a long time. The general claim of aggregators is that they create profiles of users based on their Internet behavior, but do not gather or record PII. Although we do not know that aggregators are recording PII, we demonstrate that it is undeniable that information is available to them."

"Aggregators do not have to take any action to receive this information. As part of requests, they receive OSN identifiers with pointers to the PII or in some cases, directly receive pieces of PII. This PII information can be joined with information from tracking cookies obtained from the user's traversal to any site that triggers a visit to the same aggregator. The ability to link information across traversals on the Internet coupled with the wide range of daily actions performed by hundreds of millions of users on the Internet raises privacy issues, particularly to the extent users may not understand the consequences of having their PII information available to aggregators. OSNs do have privacy policies on which OSN users rely when setting up and maintaining their account. These policies typically state that OSNs provide non-identifying information to third-parties as an aid in serving advertisements and other services. Many users, however may not understand the implications. The availability of a user's OSN identifier allows a third-party access to a user's name and other linkable PII that can identify a user. The goal of this work is not a legal examination of privacy policies, but to bring a technical examination of the observed leakage to the community's attention."

"For example, the cookie for DoubleClick.net ... means that DoubleClick can link the PII from across both MySpace and Facebook. This linkage is important because it not only allows

the aggregator to mine PII from more than one OSN, but join this PII with the viewing behavior of this user.”

The study looked at twelve social networking sites: Bebo, Digg, Facebook, Friendster, Hi5, Imeem, LinkedIn, LiveJournal, MySpace, Orkut, Twitter, and Xanga.

The authors said there were solutions to tracking: Web browsers like Firefox could be set to block access to a user’s “referrer header.” Or, third-party aggregators could filter out any PII-related headers that arrive at their servers and ensure that tracking mechanisms are clean of PII at all times.

“Third, OSNs could ensure that a wide range of privacy measures are available to members. Providing strong privacy protection by default allows an OSN to distinguish itself from other competing OSNs. Techniques at OSNs are in reality much easier. Most leakage identified in this study originated from the OSN allowing the internal user identifier to be visible to the browser unnecessarily leading to the population of the Referrer header. A straightforward solution is to strip any visible URI of user-ID information. Alternately the OSN could keep a session-specific value for the user’s identifier or maintain an internal hash table of the ID and present a dynamically generated opaque string to the browser. If the opaque string is included in the Referrer header by the browser, no information is leaked as the external site will not be able to use the opaque string to associate with the user and thus their PII,” they wrote.

(<http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf>)

### **FCRA CLASS ACTIONS: STATUTORY DAMAGES POSSIBLE WITHOUT ACTUAL DAMAGES**

A federal appeals panel has ruled that class action lawsuits under the Fair Credit Reporting Act (FCRA) need not prove actual damages in order to recover statutory damages for a willful violation of the Act. The opinion reversed a district court and aligned the U.S. Court of Appeals for the Sixth Circuit with other circuit courts that reached the same conclusion.

The case involves TeleCheck, the check-verification service used by many retailers. Because check-writers’ often don’t provide their Social Security numbers, TeleCheck relies on the driver’s license number as a primary identifier.

In 2002, Tennessee added a “zero” to the beginning of its driver’s licenses. But TeleCheck failed to account for the change, which caused its systems incorrectly to advise retailers that many Tennessee consumers had the more negative status of being first-time check-writers.

Claiming that this error affected her and “hundreds of thousands, if not millions,” of other Tennesseans, lead plaintiff Cheryl Beaudry, sought to represent a class of affected consumers, contending that TeleCheck’s “willful” failure to provide accurate information entitled class members to statutory and punitive damages and injunctive relief.

U.S. District Judge Aleta Arthur Trauger dismissed the suit, finding that FCRA plaintiffs must be able to show they incurred actual damages before they can recover statutory damages, which range from \$100 - \$1,000. The 2<sup>nd</sup> Circuit appeals panel reversed.

“The district court and the defendants suggest that, if we read the law to allow statutory damages without proof of injury, we would be creating a strict liability regime. Not so,” wrote Judge Jeffrey S. Sutton. He was joined by Judges Damon J. Keith and Helene White.

“The existence of a *willfulness* requirement proves that there is nothing ‘strict’ about the state of behavior required to violate the law. And there is an injury requirement because the statute requires the claimant to show that the defendants used unreasonable procedures in preparing a credit report about her. To the extent the defendants worry about violations of the statute that hurt no one—say a willful violation of the ‘reasonable procedures’ requirement that creates no inaccuracies in the data used to generate reports or, better yet, creates inaccuracies that *favor* the consumer—that interesting problem is not presented here. Beaudry alleges that the defendants’ systems include *false* and *negative* information about her. Under these circumstances, Beaudry’s claim should not have been dismissed,” he wrote.

Judge Sutton also said there was no Article III (i.e., Constitutional) barrier to the suit, given that Congress “has the power to create new legal rights, including rights of action whose only injury-in-fact involves the violation of that statutory right.”

“The two constitutional limitations on that power do not apply here. First, Beaudry must be “among the injured,” in the sense that she alleges the defendants violated her statutory rights. Yet that limit poses no obstacle here: Beaudry alleged that she was one of the consumers about whom the defendants were generating credit reports based on inaccurate information due to their failure to update their databases to accommodate the new Tennessee driver’s license numbering system. She thus has alleged that the defendants’ failure to follow ‘reasonable procedures to assure maximum possible accuracy’ of credit reporting information occurred ‘with respect to’ her, as the statute requires. Second, although a right created by Congress ‘need not be economic in nature, it still must cause individual, rather than collective, harm.’ The Act’s statutory damages claim clears this hurdle as well: It does not ‘authorize suits by members of the public at large,’ it creates an individual right not to have unlawful practices occur ‘with respect to’ one’s own credit information. This nexus between the individual plaintiff and the legal violation thus suffices to sustain this statutorily created right,” he wrote. (*Cheryl Beaudry, et al. v. TeleCheck Services, Inc., et al.*: CA-6 – No. 08-6428; Aug. 28.)

### **JUDGE THROWS OUT CHALLENGE TO ARREST BASED ON NO-FLY LIST**

U.S. District Judge William Alsup has dismissed discrimination claims against the city of San Francisco in a high-profile challenge to the federal government’s so-called no-fly list.

The plaintiff, Rahinah Ibrahim, had alleged the feds mistakenly placed her on the list, and that city police illegally handcuffed her at San Francisco International Airport.

That Ibrahim was a Muslim was not enough to draw an inference of discrimination under the U.S. Supreme Court's ruling last year, the judge ruled.

Judge Alsup said he was adhering to a recent U.S. Supreme Court ruling that created what lawyers refer to as a heightened pleading standard in civil cases. (see *Ashcroft v. Iqbal*, 09 C.D.O.S. 5961) But he also expressed displeasure with it.

"A good argument can be made that the *Iqbal* standard is too demanding. Victims of discrimination and profiling will often not have specific facts to plead without the benefit of discovery," Alsup wrote. "District judges, however, must follow the law as laid down by the Supreme Court."

However, Alsup wrote, Ibrahim may eventually reassert her discrimination claims – if she digs up enough facts during discovery on her surviving Fourth Amendment allegations tied to her detention at the airport. The judge barred any defense motions for summary judgment until after discovery is finished.

"Judge Alsup has created a novel way to deal with the harshness of the *Iqbal* rule," one defense lawyer, who asked for anonymity, told *The Recorder*. "Whether that's fair to defendants, or not, is something that maybe the 9th Circuit, or ultimately the Supreme Court, will decide." Another defense lawyer, San Francisco Deputy City Attorney Peter Keith, said he was confident Ibrahim will find no basis for any discrimination claim.

In *Iqbal*, a Muslim who'd been abused while incarcerated in a maximum-security prison failed to plead sufficient facts for a discrimination claim, the high court concluded. Since then, lawyers and judges have cited the case to dismiss a range of civil suits that might otherwise have survived.

Since Ibrahim, who studied at Stanford University, is a Malaysian citizen and is not currently in the United States, the Constitution does not give her the right to seek injunctive relief, Alsup wrote. "The foregoing is consistent with the recent decision of the Supreme Court holding that detainees at Guantanamo Bay may assert constitutional rights," Alsup wrote, because Guantanamo is under the control of the American government.

The judge dismissed all federal agencies and personnel from the case. Of the 400,000 individuals in the government's terrorist screening database, 3 percent of them are American citizens, according to congressional testimony offered by the Department of Homeland Security last year. The no-fly list comprises a subset of that database.

Previously, the 9th U.S. Circuit Court of Appeals reversed Judge Alsup and found that Ibrahim had standing to challenge the no-fly list.

### **SSA PAYS \$500 MILLION TO SETTLE CHARGES STEMMING FROM COMPUTER MATCHING**

The Social Security Administration (SSA) has agreed to pay an estimated \$500 million to people whose benefits it suspended or denied between January 2007 and April 2009 because of an overly-inclusive approach to computer matching. The government also agreed to change the policy under which it denies or suspends payments for people with outstanding arrest warrants.

The lawsuit revolved around the SSA's policy for suspending or denying benefits for people with outstanding felony warrants. The plaintiffs argued the policy went beyond a provision in the Social Security Act designed to prevent people from using Social Security money to flee prosecution. For instance, one plaintiff allegedly bounced a check in Texas and was unaware of his outstanding warrant until his disability benefits were cut off.

Plaintiffs also argued that the government's use of a computer system that matched names in warrant databases to those at the Social Security Administration led to people without any outstanding warrants being denied their benefits. Plaintiff Rosa Martinez, for example, sought help from Legal Aid Society of San Mateo after her benefits were cut off due to an outstanding warrant for another woman with the same name.

Under a proposed settlement preliminarily approved by Judge Claudia Wilken, the SSA agreed to narrow its policy to warrants issued on charges such as flight or escape.

Various attorneys representing plaintiffs said the SSA had litigated the key issue in the case – the interpretation of the statute dealing with government benefits to those fleeing arrest – in individual cases and lost eight times. People whose benefits were denied or suspended between 2000 and 2006 also will have a chance to reinstate their benefits.

### **NY TIMES CAN'T OBTAIN SPITZER WIRETAP DATA, COURT RULES**

A federal appeals panel has rejected the *The New York Times* bid to obtain wiretap information related to former New York Gov. Eliot Spitzer's involvement in a prostitution ring.

While federal wiretap law permits disclosure of wiretap information on a showing of "good cause," news media's interest in publishing the information did not qualify, the 2nd U.S. Circuit Court of Appeals ruled August 7th. The panel, consisting of Judges Ralph K. Winter, Jose A. Cabranes and Peter W. Hall, also ruled that the *Times* did not have a First Amendment right to gain access to wiretap applications and related documents.

The decision overturns a ruling by Southern District of New York Judge Jed S. Rakoff, who granted the Times' application to access sealed wiretap applications in the Emperor's Club investigation.

In *National Broadcasting Co. v. U.S. Dept. of Justice*, 735 F.2d 51 (1984), the 2nd Circuit concluded that "'good cause' could be found where the applicant seeking to unseal wiretap applications was an 'aggrieved person,' but not upon a lesser showing, Judge Cabranes wrote. In NBC, he said, the court found a presumption against disclosure of both the fruits of wiretap surveillance and the wiretap applications. The circuit ruled then that NBC was not an "aggrieved person" because, in the words of Title III, it was not "a party to any intercepted wire or oral communication or a person against whom the interception was directed." The same principle applied to this case, he concluded. *In the Matter of the Application of the New York Times Co. To Unseal Wiretap & Search Warrant Materials*: CA-2 – 09-0854-cv.

**FOIA CT. ROUNDUP: CUSTOMS VAUGHN;  
PRIVACY FOR HUD COMPLAINANT?**

The following is a summary of recent court decisions under the Freedom of Information Act.

***Citizens for Responsibility & Ethics in Wash. v. Dept. of Homeland Security***: (No. 08-1046)

**Court:** U.S. District Court for the District of Columbia  
**Judge:** John D. Bates  
**Exemption:** FOIA (b)(5), deliberative process privilege, attorney-client privilege  
**Documents:** Communications with Ray Hunt regarding U.S.-Mexico border fence  
**Issue:** Adequacy of *Vaughn* index  
**Date:** September 1, 2009

In a mixed opinion, the court ruled that the U.S. Customs and Border Protection (CBP) failed to justify withholding under Exemption 5 of some documents that were created as part of the agency's effort to counter allegations in a *Texas Observer* article that Ray L. Hunt received preferential treatment relating to the placement of the U.S.-Mexico border fence.

Citizens for Responsibility and Ethics in Washington (CREW) requested all communications between Ray Hunt and CPB.

Judge John D. Bates said a declaration by, Mark Hanson, Director of the FOIA Division at CBP's Office of International Trade, contained "only three paragraphs that addressed the applicability of Exemption 5 to the disputed documents: (1) protection of chains of e-mail messages that detail CBP's internal deliberations revealing both the deliberative-thought process of CBP individuals and the overall decision-making process of CBP as an agency;" (2) protection of "the normal back-and-forth" deliberations regarding allegations of improper preferential treatment being afforded Ray L. Hunt; and (3) protection of deliberations regarding what should, and should not, have been included in the final version of the document.

But the declaration was not adequate, he ruled. “The Court is unable to determine whether these documents have been properly withheld due to the lack of detail in CBP’s *Vaughn* submission. After examining unredacted copies of these documents *in camera*, critical information remains missing – including, for example, the documents’ respective authors, recipients, purposes or uses – that is not evident from the face of the documents themselves. Without such details, the Court cannot assess what role these documents played in the decisionmaking process and, ultimately, whether Exemption 5 applies. Moreover, CBP’s characterization of these documents as ‘drafts’ or ‘talking points’ is, without more, insufficient to establish that they are both ‘predecisional’ and ‘deliberative.’ The Court also notes that there appears to be a significant amount of purely factual material contained in these documents and such information is generally subject to disclosure,” he wrote, noting that a “segregability” analysis was also missing.

The Customs agency also sought to invoke the attorney-client privilege for a document marked “Per OCC,” which it belatedly clarified stood for Office of Chief Counsel. But after an *in camera* review, Judge Bates said the redacted material did not contain confidential client information, nor did it solicit legal advice – “it merely acknowledges that legal advice will be given in the future.”

“Because the attorney-client privilege covers ‘confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice,’ this material is not protected by the privilege and it must be released,” he wrote.

**Prudential Locations v. Dept. of Housing and Urban Development:** (No. 09-00128)

**Court:** U.S. District Court for the District of Hawaii  
**Judge:** Susan Oki Mollway  
**Exemption:** FOIA (b)(6), privacy  
**Documents:** Identities of complainant regarding Prudential  
**Issue:** Privacy vs. public interest when complainant is allegedly malicious  
**Date:** July 27, 2009

The court ruled that Dept. of Housing and Urban Development (HUD) properly withheld the identities of a person or persons who complained to the agency of alleged violations by Prudential Locations.

Prudential said the identities must be disclosed because those complaining to HUD were maliciously accusing it without a basis and therefore did not deserve privacy.

But Chief Judge Susan Oki Mollway disagreed. “The identities of the individuals filing complaints with HUD do not shed any light on the agency’s activities. All of the factual allegations in the investigations are available to the public; anyone wishing to challenge the accuracy of the allegations need only attack the factual bases of the complaints. As the Ninth Circuit recently held in a FOIA request for the identities of individuals involved in an agency investiga-

tion, ‘We are not persuaded that direct contact with the individuals would produce any information that has not already been revealed to the public.’” (see *U.S. Forest Serv.*, 524 F.3d at 1028)

“Here, there is no suggestion that the motives of the individuals involved affected the outcome of the HUD investigation or somehow biased the agency ... Prudential does not maintain that the investigators themselves are guilty of wrongdoing; even if a complaint is filed maliciously, the agency may evaluate the facts fairly and reach a just conclusion. The Ninth Circuit recently explained that “the evidence must show some nexus between the specific requested information and unveiling agency misconduct--the public interest advanced here.” (see *Lahr*, 569 F.3d at 978.) There is no indication that the identity of the informant would reveal any misconduct by HUD. Nor do the disclosure requirements in FOIA turn on the accuracy of information given by private individuals. Stronger than any public interest in disclosure of any informant’s identity is the public’s interest in encouraging the reporting of RESPA violations and in uncovering agency misconduct,” she wrote.

“Prudential’s own plans to use this information are not the sole basis for evaluating the invasion of privacy. The court must ‘evaluate both the public benefit and the potential invasion of privacy by looking at the nature of the information requested and the uses to which it could be put if released to any member of the public.’”

#### **Exemption 4**

Judge Harold H. Kennedy, Jr. ruled that the Federal Motor Carrier Safety Administration (FMCSA) properly redacted under Exemption 4 confidential commercial and financial information from three FMCSA decisions. The decisions concerned applications for self-insurance authorization. (*Jeremy Kahn v. FMCSA*: USDC-D.C. – No. 07-02323; Aug. 26.)

#### **IN BRIEF . . .**

##### **Court Orders ID of Anonymous Blogger**

Canadian model Liskula Cohen was able to identify an anonymous blogger who attacked her because a Manhattan judge ordered Google to disclose the blogger’s identity. Cohen, 36, claimed the blogger defamed her by posting words like “skanky,” “ho”, and “whoring” below her photographs at blogger.com, which is owned by Google. Google initially refused to unmask the unidentified writer. But Justice Joan Madden of the New York State Supreme Court rejected the blogger’s argument that “blogs serve as a modern day forum for conveying personal opinions, including invective and ranting, and that the statements in this action when considered in that context, cannot be reasonably understood as factual assertions.” The IP address turned over by Google revealed that the blogger was an acquaintance of Cohen’s. Cohen and her lawyer, Steven Wagner, told ABC News they were planning a defamation suit against the blogger.

Matt Zimmerman, senior staff attorney at the Electronic Frontier Foundation, expressed concern over the precedent. "The notion that you can use the court as your personal private investigator to out anonymous critics is a dangerous precedent to set. This doesn't change the rules ... but I think the practical impact is that litigious people will see this as a green light to try to out critics. It's one of those bad facts make bad law cases."

**FTC Settles Safe Harbor Charges**

A California company has agreed to stop tricking consumers into believing that they were buying electronics from a company operating in the United Kingdom that complied with U.S./E.U. Safe Harbor agreement for protecting personal data. The accord was the product of a Federal Trade Commission complaint that also accused the company and its owner of falsely saying that manufacturer warranties for its products were valid in the UK. The Pasadena-based defendants charged in the case are Balls of Kryptonite, doing business as Best Priced Brands and Bite Size Deals, and its owner, Jaivin Karnani. Their Web sites were [www.bestpricedbrands.co.uk](http://www.bestpricedbrands.co.uk) and [www.bitesizedeals.co.uk](http://www.bitesizedeals.co.uk). ([www.ftc.gov/opa/2009/08/bestpriced.shtm](http://www.ftc.gov/opa/2009/08/bestpriced.shtm))

**Banking on Thumbprints**

A man with no hands could not cash a check at Bank of America branch in Tampa, Flor. because he could not provide a thumbprint. The reason: Steve Valdez was born without arms and wears prosthetic devices. The check was written on his wife's Bank of America check, which had the same address he has on his driver's license. Valdez showed two ID cards – both with pictures. The branch manager suggested he either bring in his wife or open an account, which Valdez refused to do. A spokesman for Bank of America told WTSB-TV News that despite the thumbprint requirement the bank should have made accommodations for Valdez.

---

**YES** I Want To Subscribe & Save 10% Off The \$390 Annual Rate

\_\_\_\_\_ \$350 Per Year (23 Issues)  
\_\_\_\_\_ \$670 2-Year (46 issues)

Name \_\_\_\_\_

Org. \_\_\_\_\_

Address \_\_\_\_\_

City/ST/ZIP \_\_\_\_\_

\_\_\_\_\_ Credit Card No. (Visa, MC or Amex)

Phone No. \_\_\_\_\_

\_\_\_\_\_ Expiration Date

(Or you can pay by Check or Purchase Order)

**Privacy Times**

P.O. Box 302

Cabin John, MD 20818

(301) 229-7002 [Ph] (301) 229-8011 [Fax]