PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Volume 31 Number 5 March 2, 2011

CAPITAL INSIGHTS: Sen. Al Franken (D-MN) is the new chairman of the Senate Judiciary's Subcommittee on Privacy, Technology and the Law. In announcing Franken's position, Committee Chairman Patrick Leahy (D-VT) said he "looked forward to continued progress in protecting Americans' personal privacy." Last year, Franken was one of several Senators to urge Facebook to fix its privacy policy to block users' personal information from being accessed by third parties without the users' consent. Sen. Tom Coburn (R-OK) will serve as the panel's ranking member. Other Democratic members include Chuck Schumer (NY), Sheldon Whitehouse (RI) and Richard Blumenthal (CT). Republican members include Orrin Hatch (UT) and Lindsey Graham (SC). . . . Revelations that Google was gathering children's Social Security numbers, dates of birth and birthplace on its "Doodle 4 Google" contest entry forms has prompted Consumer Watchdog to call on the House Commerce Committee to hold hearings and investigate. In the contest, the company invites "K-12 students to use their artistic talents to think big and redesign Google's homepage logo for millions to see." Committee Chairman Joe Barton (R-TX) and Ranking Member Ed Markey called the practices "sketchy," and indicated they would hold hearings on the matter. Simpson said there was "no legitimate business reason to gather such sensitive information about children." Noting that the FTC had closed an earlier probe of Google because it as satisfied the company had made privacy improvements, Simpson asked the committee to investigate those changes as well.

MAJOR STORIES IN THIS ISSUE

'PERSONAL' PRIVACY EXEMPTION IS FOR INDIVIDUALS, NOT 'LEGAL PERSONS'

Rejecting AT&T Corp.'s bid to block disclosure, the U.S. Supreme Court ruled 8-0 that the Freedom of Information Act's privacy exemption ["7(C)"] for law enforcement files only applied to humans and did not extend to corporations. The opinion reflected the justices' disdain for AT&T's arguments by concluding, "We trust that AT&T will not take it personally."

Reversing the Third Circuit, the High Court dismissed AT&T's argument that because a corporation like itself was a "legal person," it qualified for Exemption 7(C)'s protection for *personal* privacy. Prior to the ruling, some observers speculated that since the Court last year upheld corporations' "free speech" rights under the First Amendment in its controversial ***Citizens United*** ruling, it also would be inclined to recognize a corporate "right to privacy."

But this case was about the FOIA statute, not constitutional rights, the court said. "AT&T contends that this Court has recognized 'privacy' interests of corporations in the Fourth Amendment and double jeopardy contexts, and that the term should be similarly construed here. But this case does not call upon us to pass on the scope of a corporation's 'privacy' interests as a matter of constitutional or common law. The discrete question before us is instead whether Congress used the term 'personal privacy' to refer to the privacy of artificial persons in FOIA Exemption 7(C); the cases AT&T cites are too far a field to be of help here," wrote Chief Justice John Roberts.

The unanimous opinion included a detailed discussion on language and its statutory construction within the FOIA.

"'Person' is a defined term in the [FOIA] statute; 'personal' is not. When a statute does not define a term, we typically 'give the phrase its ordinary meaning.' 'Personal' ordinarily refers to individuals. We do not usually speak of personal characteristics, personal effects, personal correspondence, personal influence, or personal tragedy as referring to corporations or other artificial entities. This is not to say that corporations do not have correspondence, influence, or tragedies of their own, only that we do not use the word 'personal' to describe them," he wrote.

"Although the question whether Exemption 6 is limited to individuals has not come to us directly, we have regularly referred to that exemption as involving an 'individual's right of privacy.'" Chief Justice Roberts wrote, citing ***Dept. of State v. Ray***, 502 U. S. 164, 175 (1991), ***Dept. of Air Force v. Rose***, 425 U. S. 352, 372 (1976); and ***Dept. of State v. Washington Post Co.***, 456 U. S. 595, 599 (1982).

"In drafting Exemption 7(C), Congress did not, on the other hand, use language similar to that in Exemption 4. Exemption 4 pertains to 'trade secrets and commercial or financial information obtained from a person and privileged or confidential.' This clearly applies to corporations—it uses the defined term 'person' to describe the source of the information—and we far more readily think of corporations as having 'privileged or confidential' documents than personally private ones. So at the time Congress enacted Exemption 7(C), it had in place an exemption that plainly covered a corporation's commercial and financial information, and another that we have described as relating to 'individuals.' The language of Exemption 7(C) tracks the latter," he wrote.

"Regardless of whether 'personal' can carry a special meaning in legal usage, 'when interpreting a statute we construe language in light of the terms surrounding it.'"

"Exemption 7(C) refers not just to the word 'personal,' but to the term 'personal privacy.' AT&T's effort to attribute a special legal meaning to the word 'personal' in this particular context is wholly unpersuasive."

"AT&T's argument treats the term 'personal privacy' as simply the sum of its two words: the privacy of a person. Under that view, the defined meaning of the noun "person," or the asserted specialized legal meaning, takes on greater significance. But two words together may assume a more particular meaning than those words in isolation. We understand a golden cup to be a cup made of or resembling gold. A golden boy, on the other hand, is one who is charming, lucky, and talented. A golden opportunity is one not to be missed. 'Personal' in the phrase 'personal privacy' conveys more than just 'of a person.' It suggests a type of privacy evocative of human concerns—not the sort usually associated with an entity like, say, AT&T," Justice Roberts continued.

Despite its contention that 'common legal usage' of the word 'person' supports its reading of the term 'personal privacy,' AT&T does not cite a single instance in which this Court or any other (aside from the Court of Appeals below) has expressly referred to a corporation's 'personal privacy.' Nor does it identify any other statute that does so. On the contrary, treatises in print around the time that Congress drafted the exemptions at hand reflect the understanding that the specific concept of 'personal privacy,' at least as a matter of common law, did not apply to corporations.

"AT&T contends that this Court has recognized 'privacy' interests of corporations in the Fourth Amendment and double jeopardy contexts, and that the term should be similarly construed here. But this case does not call upon us to pass on the scope of a corporation's 'privacy' interests as a matter of constitutional or common law. The discrete question before us is instead whether Congress used the term 'personal privacy' to refer to the privacy of artificial persons in FOIA Exemption 7(C); the cases AT&T cites are too far a field to be of help here."

"AT&T concludes that the FCC has simply failed to demonstrate that the phrase 'personal privacy' 'necessarily excludes the privacy of corporations.' But construing statutory language is not merely an exercise in ascertaining 'the outer limits of a word's definitional possibilities,' AT&T has given us no sound reason in the statutory text or context to disregard the ordinary meaning of the phrase 'personal privacy.'"

"The meaning of 'personal privacy' in Exemption 7(C) is further clarified by the rest of the statute. Congress enacted Exemption 7(C) against the backdrop of pre-existing FOIA exemptions, and the purpose and scope of Exemption 7(C) becomes even more apparent when viewed in this context." (***Federal Communications Commission et al;. v. AT&T Inc. et al.***: U.S. Supreme Court – No. 09–1279; March 1.)

HUNTON & WILLIAMS, 'PRIVACY EXPERT,' SNARED IN INVASION-OF-PRIVACY SCANDAL

A major law firm that perennially has won a so-called "Best Privacy Adviser" award, is embroiled in an invasion-of-scandal and the target of a complaint to the District of Columbia Bar Association for violating the code of legal ethics.

The controversy stems from a proposed campaign involving Hunton & Williams to discredit both the liberal opponents of the U.S. Chamber of Commerce and the supporters of WikiLeaks through collection of personal data and dirty tricks.

The Feb. 23rd bar complaint, filed by the group "StopTheChamber" against Hunton & Williams Partners John W. Woods, Richard L. Wyatt Jr., and Robert T. Quackenboss, accuses the attorneys of being involved in a conspiracy to filch data from the Facebook sites of the Chamber's political critics – and their families and children – in possible violation of federal law.

The alleged conspiracy, reportedly involving Hunton & Williams and private security companies Palantir, HBGary Federal and Berico Technologies – collectively known as "Team Themis" – came to light because of e-mails leaked by "Anonymous." "Anonymous" reportedly hacks the e-mail and data systems of organizations that attack groups it supports, like WikiLeaks and StopTheChamber.

The leaked e-mails indicated that as part of an effort to win a $2 million contract with Hunton & Williams, Aaron Barr, an executive at HBGary. circulated numerous e-mails and documents detailing information about political opponents' children, spouses, and personal lives.

One of the targets was Mike Gehrke, a former staffer with "Change to Win." Among the information circulated about Gehrke was the specific "Jewish church" he attended and a link to pictures of his wife and two children. (Portions of these e-mails, with sensitive information redacted by the group "ThinkProgress," are available at: http://thinkprogress.org/2011/02/10/chamberleaks-target-families/. Many of the leaked e-mails are at http://search.hbgary.anonleaks.ch/.)

Another target was Brad Friedman, co-founder of "The Brad Blog." Barr's profile of Freidman included information about his "life partner" and his home address.

"This tactic of targeting opponents' personal lives and family was not simply a random event," wrote ThinkProgress. "Rather, it was a concerted and deliberate effort to use anything possible to smear the Chamber's political opponents. To dramatize his firm's intimidation tactics, Barr sent an e-mail to Hunton & Williams Partner John Woods that contained personal details about fellow Hunton attorney Richard Wyatt, who was representing the Chamber. The e-mail was intended to show Woods and Wyatt "how 'vulnerable' they are."

The e-mail posted by ThinkProgress shows Barr stating, "BTW, might want to tell Richard to have his wife [redacted name] hide her friends list. He doesn't seem to have a presence in social media (besides a very old LinkedIn account, but [wife's name redacted] has enough to profile her to him based about 20 min. of analysis. I would recommend adding a brief training course for partner/employees on the state of the art for social media analysis and how people and systems can be exploited using social media. As an example. Richard probably has a network at home. Richard and [wife's name redacted] probably share the same network, maybe even the same computer. Either way, If I can exploit her account through one of her social connections, I can exploit the home network/system. Lots of vulnerabilities in social media but first step is reducing your exposure for someone to identify you as a target."

Facebook and LinkedIn specifically prohibit the use of software programs to harvest information from their sites. For example, Facebook states: "You will not collect users' content or information, or otherwise access Facebook, using automated means such as harvesting bots, robots, spiders, or scrapers without our permission.") (https://www.facebook.com/terms.php)

The Bar complaint cites both Facebook's and LinkedIn's policies, and goes on to allege that Robert Woods and his firm Hunton & Williams may have conspired with Themis to commit "identity theft" in violation of the "Digital Millennium Copyright Act, 18 U.S.C. § 2511 (intercepting electronic communications), 18 U.S.C. § 2701 (accessing stored communications), and 18 U.S.C. § 1030(a)(2) (accessing a computer and obtaining information)."

For the past four years, Hunton & Williams has won *Computerworld's* "Best Privacy Advisers" award, based on a "survey of more than 4,000 global corporate privacy leaders, citing the firm's extensive experience and global presence."

The firm's privacy specialists include Paula Bruening (formerly of the Center for Democracy & Technology), Marty Abrams (formerly of Experian) and Indiana Law Professor Fred Cate. International specialists include Lisa J. Sotto (New York), Christopher Kuner (Brussels) Bridget C. Treacy (London). Neither these specialists, nor the law firm, responded to *Privacy Times'* request for a comment.

The deal never happened, according to the U.S. Chamber of Commerce. *Legal Times* reported that the Chamber said in a statement that it knew nothing of the proposals and never made any payments for them. "No money, for any purpose, was paid to any of those three private security firms by the Chamber, or by anyone on behalf of the Chamber, including Hunton and Williams," the Chamber said.

NLRB SETTLES WITH COMPANY OVER 'FACEBOOK FIRING'

A Connecticut ambulance company has settled a lawsuit brought by the U.S. National Labor Relations Board (NLRB) involving the firing of an employee who had published negative remarks about her boss on her Facebook page.

A lawsuit filed by the NLRB against American Medical Response of Connecticut Inc. (AMR) on October 27, 2010, argued that the company illegally terminated Dawnmarie Souza for criticizing her supervisor on her personal Facebook page. The NLRB said Souza's negative comments were protected speech under federal labor laws.

The lawsuit also alleged that AMR illegally denied union representation to the employee during an investigatory interview, and maintained and enforced an "overly broad" blogging and Internet posting policy that "contained unlawful provisions."

Souza wrote on her Facebook page, "Love how the company allows a 17 to be a supervisor," referring to AMR's code for a psychiatric patient, and called her boss a "scumbag as usual," using her home computer, after she was denied the right to seek union help before she responded to a supervisor's questions about a customer complaint.

AMR said it had fired her following complaints about her work. Souza served as an emergency medical technician for the company.

The case has received widespread attention for its groundbreaking attempt to set legal limits on employers' Internet policies. The financial terms of the settlement were not disclosed but workplace policy reforms were detailed.

Under the settlement, AMR has agreed to change its blogging and Internet policy that barred workers from making disparaging remarks against the company or their supervisors. The company also will revise another policy that prohibited employees from depicting the company in any way over the Internet without permission.

Both policies prevented AMR workers from discussing wages, hours and working conditions with others, the NLRB said.

"Under the settlement approved by Hartford Regional Director Jonathan Kreisberg, Souza didn't get her job back, but AMR agreed to revise its 'overly broad rules' to ensure that they do not improperly restrict employees from discussing their wages, hours and working conditions with co-workers and others while not at work, and that they would not discipline or discharge employees for engaging in such discussions," the NLRB said in a statement.

The company will no longer deny employee requests for union representation when meeting with managers. Moreover, employees, who request union representation, would no longer be threatened with discipline, according to the agency, the agency said. Souza said she has no intentions of rejoining the company.

In Brief . . .

$4.3 Million HIPAA Fine

The U.S. Dept. of Health and Human Services has fined Cignet Health $4.3 million for denying patients access to their records in violation of the Health Insurance Portability and Accountability Act (HIPAA) privacy rules. It was first civil money penalty that HHS's Office of Civil Rights has imposed under the HIPAA rule since it took effect in 2003. Cignet Health is a health plan and also operates two clinics offering services, such as family practice and some specialties, in Prince George's County, a suburb of Washington, D.C. OCR found that Cignet violated the rights of 41 patients by denying them access to their medical records when they requested them during the period between Sept. 2008 and Oct. 2009. The patients individually filed complaints with OCR, initiating investigations of each complaint. HHS made the determination against Cignet in October, but announced the fine Feb. 22nd. The HIPAA privacy rule requires that a covered entity, such as a healthcare provider or health plan, supply a patient with a copy of their medical records within 30 days, and no later than 60 days of the patient's request.

Cignet also was fined for refusing to cooperate with OCR's investigations by not responding to demands for records from March 17, 2009, to April 7, 2010. OCR filed a petition to enforce its subpoena in U. S. District Court and obtained a default judgment against Cignet on March 30, 2010. On April 7, Cignet produced the medical records to OCR, but otherwise made no efforts to resolve the complaints through informal means. OCR said it will continue to investigate and take action against organizations that knowingly disregard their obligations.

FOIA & 'Metadata'

U.S. District Judge Shira Scheindlin ruled for the first time that federal agencies must disclose "metadata" under the Freedom of Information Act (FOIA). While stating there were too many variable to set a hard rule, she wrote, "The best way I can answer the question is that metadata maintained by the agency as part of an electronic record is presumptively producible under FOIA, unless the agency demonstrates that such metadata is not 'readily reproducible.'"

"Metadata" is a broad term essentially defined as data providing information about one or more aspects of other data, including their: (1) means of creation; (2) purpose; (3) time and date of creation; (4) creator or author, or (5) placement on a computer network, or (6) standards used. The case involved the National Day Laborer Organizing Network's bid for information on a collaborative program between ICE, the Justice Dept. and States and localities for enforcement

of federal immigration law. Cooperation broke down when ICE disregarded NDLON's request for electronic format and only provided PDF files. Judge Scheindlin dismissed as a "lame excuse" the government's argument that NDLON failed to specify the format it wanted. She noted the Network attorney's e-mail explicitly placed Defendants on notice that spreadsheets were sought in native format – not as a PDF screen shot – and that each text record should be produced as a separate file. Judge Scheindlin did curb the scope of disclosure, stating that "while native production is often the best form of production, it is easy to see why it is not feasible where a significant amount of information must be redacted." (***National Day Laborer Organizing Network v. U.S. Immigration & Customs Enforcement Agency***: USDC-S.D.N.Y. – No. 10 Civ. 3488; Feb. 7.)

FOIA Search

Judge Ricardo Urbina ordered the U.S. Customs and Border Protection (CBP) to conduct an adequate search for records on a convicted heroin dealer. "Because CBP may not 'limit its search to only one record system if there are others that are likely to turn up the information requested,' and because CBP has not demonstrated that responsive documents would not reasonably be found in other record systems or that it searched any other potential sources but found no responsive records, the court determines that CBP has not demonstrated that its search was adequate." According to Shari Suzuki, CBP's Chief of FOIA appeals, said the agency responded to the FOIA request by searching its Treasury Enforcement Communications System database (TECS), using Plaintiff Miguel Concepcion's name and date of birth as search terms. (***Alberto Concepcion v. U.S. Customs and Border Protection***: USDC-D.C. – No. 10-0599; March 3.)