Privacy Times Copyright © 2000

Volume 20 Number 14, July 26, 2000

*CAPITAL INSIGHTS: Privacy continues to whirl through Washington. . . . The Federal Trade Commission settled with ToySmart, forcing the bankrupt e-tailer to abandon plans to sell customer information that was collected under a promise not to. But Commissioners Sheila Anthony and Orson Swindle dissented, arguing that the "bundling" deal didn't go far enough to protect privacy. (www.ftc.gov/opa/2000/07/toysmart2.htm) . . . . The FBI told the House Judiciary Subcommittee on the Constitution it has only used "Carnivore," its e-mail surveillance program, in 25 cases in the past two years. But several civil libertarians, technologists and industry reps criticized the system as a major threat to communications privacy. The ACLU has filed a FOIA suit, trying to force the FBI to release more details, including Carnivore's "source code." Republican Majority Leader Richard Armey (TX) said Carnivore should be suspended until the concerns of privacy advocates and the needs of law enforcement are reconciled. Despite tough questioning, Subcom. Chairman Charles Canady (R-FL) and other lawmakers seemed reluctant to force the program's suspension immediately. www.house.gov/judiciary/2.htm . . . . Canady joined Rep. Bob Barr (R-GA) to introduce a bill to require employers notify workers there are monitored electronically. Sen. Charles Schumer (D-NY) sponsored the Senate bill. . . . The House Ways & Means Subcommittee on Social Security July 20 approved a bill (HR 4587) to clamp down on the sale of Social Security numbers and halt their display on drivers' licenses and other government documents. The bill could be doomed by its late start, but has picked up some momentum, as lawmakers scramble to show they're doing something to guard privacy. . . . However, a 10-10 vote in the Senate Banking Committee blocked an effort by Sens. Richard Shelby (R-AL) and Richard Bryan (D-NV) to ban financial institutions from selling SSNs. Their target was a measure (S 2107) on SEC fees. Banking Chairman Phil Gramm (R-TX) led the fight against the privacy measure. . . . Microsoft, AOL, RealNetworks, Intel -- all firms that have committed privacy blunders -- have joined with 32 other companies to form "Privacy Partnership 2000." The consortium will fund print, radio and Web ads to "educate" the public and offer tips. Organized by TRUSTe, the effort is aimed at convincing the public that the group's seal guarantees adequate privacy, a notion that advocates like Jason Catlett, of Junkbusters, scoffed at. . . . **Late Flash:** OMB is seeking comments for a study on bankruptcy and privacy. Contact: USTPrivacyStudy@usdoj.gov*

MAJOR STORIES IN THIS ISSUE

IDENTITY THEFT ON RISE, SAYS FTC OFFICIAL; EMPLOYEES TARGETED BY IDENTITY THIEVES

The rise in identity theft may be accelerating because of a disturbing new trend, "group identity theft," in which perpetrators target the workplace for its trove of personal information, and dozens of people find themselves victimized by a single offender or a ring of thieves. In California, an employee lawsuit is pending against a drug company where their data was stolen.

In another recent case of "group identity theft," the San Diego office of Ericsson, the wireless company, two identity thieves used employee data culled from personnel records to access online stock trading accounts and then drain funds. They also opened credit cards using employees' identities.

According to reports in the July 23 *San Diego Union Tribune*, Jeanette L. Franklin, 29, a payroll employee at Ericsson's Richardson, Texas, headquarters, and an accomplice, Babatunde Osiname, 35, have been arrested and charged with taking personal information and draining funds from employees' E*Trade stock accounts. Franklin was arrested and appeared in Federal court in Dallas July 19.

According to reports, at least eight employees were victimized and nearly $700,000 was taken from bank accounts, including $285,000 from one account. In that case, the perpetrators were able to gain control of the account by calling E*Trade, providing the employee's name and Social Security number, and then gaining the password and taking control of the account.

Furthermore, at least 25 additional employees had credit cards opened in their names by an unknown perpetrator. Money from those accounts was used for online stock trading; charges to those cards were reported to reach $840,000.

Meanwhile, before a July 12 Congressional hearing, Jodi Bernstein, director of the FTC's Bureau of Consumer Protection, told the Senate Judiciary Committee's Subcommittee on Technology, Terrorism and Government Information that its information hotlines are deluged with calls and that identity theft has gripped the public like no previous consumer issue. FTC phone counselors are handling 850 calls per week and have taken more than 20,000 calls in the past eight months. They advise identity theft victims on specific steps they can take to minimize additional harm to their finances and credit, Bernstein said.

Based on callers' information, the FTC has compiled the following statistics on identity theft: Approximately 54 percent of consumers reported credit card fraud - a credit card account opened in their name or a "takeover" of their existing credit card account; Approximately 26 percent reported telephone, cellular, or other utility service opened in their name by the identity thief; 16 percent reported that a checking or saving account had been opened in their name, and/or that fraudulent checks had been written; and approximately 11 percent reported that the identity thief obtained loans in their name.

California, New York, Florida, Illinois and Texas—States with the largest populations—had the largest number of identity fraud cases.

FTC data also yielded information about perpetrators. Almost 60 percent of the callers could provide some identifying information about the thief, including a name, address or phone number, and more than 25 percent of callers said they knew the thief personally. Damage costs range greatly with 34 percent of cases involving less than $1,000; 35 percent totaling $1,000 to $5,000; 13 percent totaling between $5,000 and $10,000; and 18 percent over $10,000.

Bernstein testified that the FTC will begin to share its information with law enforcement agencies as well as businesses "whose practices are frequently associated with identity theft." An FTC workshop for consumer groups and law enforcement agencies on identity theft is scheduled for the fall.

The subcommittee is not expected to act—if at all—on testimony from the hearing until after the August recess, informed sources told *Privacy Times.*

Mari L. Frank, a San Diego attorney representing employees who had personal information stolen in the workplace, told *Privacy Times* that although state and federal statutes against identity theft exist, employers are not doing enough to protect employees' personal information.

"The workplace has become a hotspot for consumers to become the victims of identity thieves," she said. "The issue is proper information handling practices in the workplace."

Frank, who herself has been victimized by identity theft, is representing a group of scientists from the San Diego-based pharmaceutical company Ligent who had their personal information stolen and used to open credit cards, obtain telephone lines and other services. In the Ligent case, a lab technician with previous convictions for fraud stole employee payroll information. The records were kept in a storage space accessible to all employees.

The employee took records out of the office, sold them to friends and used them herself. 100 victims have been identified. Frank's clients contacted her last October after learning that their colleagues were all experiencing credit card fraud.

"In January, they contacted the company and said 'There are a bunch of us who are victims who all work for you.' The company said, 'Well, it has nothing to do with us. Our HR department is secure,'" Frank said. After an investigation by the U.S. Secret Service, the suspect was arrested in March. Plaintiffs are currently in settlement negotiations with Ligent.

This year, several executives at General Motors got hit when a temporary employee sold their personnel records. Clerks at a national department store recently complained they were all getting harassing phone calls from debt collectors, a firm indication of an identity fraud cluster.

The Los Angeles Times reported July 16 that a dozen teachers at Webster Middle School in West Los Angeles are pushing law enforcement to consolidate its cases and pursue the

perpetrators. One teacher, Lorraine Machado, also is urging credit grantors to investigate -- not just to clear her name, but to find the crooks who stole her identity. The teachers began comparing notes when one overheard another on the phone complaining to a debt collector that she was not responsible for the debts. Some suspect that an employee in the headquarters of the L.A. Unified School District filched names and SSNs from a central computer.

Last year, it is estimated that more than 750,000 people were victims of identity theft, Frank said. "[Credit bureau] Trans Union logged more than 62,000 calls per month in 1999," Frank said. "Identity theft is a very easy crime to commit," she said. "There are not a lot of investigative resources, you can commit the crime and not risk getting caught, and if you get caught, you probably won't do much time," she added.

Ted Leventhal

FCRA: NINTH CIRCUIT REVERSE IN ANDREWS; BANK LIABILITY

A federal appeals panel in San Francisco July 17 made a pro-consumer ruling in a Fair Credit Reporting Act, ordering a jury to decide whether TRW's (now Experian's) procedures for ensuring accuracy were adequate in light of the growth in identity theft, and whether it should have to pay punitive damages.

Reversing a lower court, the U.S. Court of Appeals for the Ninth Circuit also ruled for the first time that the FCRA's statute of limitations begin to toll when the consumer learns of a mistake related to her credit report, and not when the mistake actually occurred. The holding conflicts with decisions of the Third, Fifth, Seventh, Tenth and Eleventh Circuits.

The decision stems from a suit brought by Adelaide Andrews, a California woman, who learned that her Social Security number (SSN) was stolen by her doctor's receptionist, Andrea Andrews. The imposter applied for, and obtained credit using Adelaide's SSN. Adelaide sued Trans Union and TRW for disclosing her credit report to creditors. Trans Union settled the case.

U.S. District Lourdes Baird, of Los Angeles, ruled there was no violation of FCRA disclosure provisions (Sect. 1681b), finding that the law permits release of a credit report when the consumer is "involved" in the transaction. Since the imposter used Adelaide's SSN, Adelaide was involved, she reasoned.

The appeals panel disagreed. "'Involve' has two dictionary meanings that are relevant: (1) 'to draw in as a participant' or (2) 'to oblige to become associated.' The district court understood the word in the second sense. We are reluctant to conclude that Congress meant to harness any consumer to any transaction where any crook chose to use his or her number. The first meaning of the statutory term must be preferred here. In that sense the Plaintiff was not involved," wrote Judge John T. Noonan. He was joined by Judges William Canby Jr. and William A. Fletcher.

"As the district court observed, there are 250 million persons in the United States (not all of them having Social Security numbers) and 1 billion possibilities as to what any one Social

Security number may be. The random chance of anyone matching a name to a number is very small. If TRW could assume that only such chance matching would occur, it was reasonable as a matter of law in releasing the Plaintiff's file when an application matched her last name and the number. But we do not live in a world in which such matches are made only by chance."

"We take judicial notice that in many ways persons are required to make their SSNs available so that they are no longer private or confidential but open to scrutiny and copying. Not least of these ways is on applications for credit, as TRW had reason to know. In a world where names are disseminated with the numbers attached and dishonest persons exist, the matching of a name to a number is not a random matter. It is quintessentially a job for a jury to decide whether identity theft has been common enough for it to be reasonable for a credit reporting agency to disclose credit information merely because a last name matches a SSN on file," the court said.

"In making that determination the jury would be helped by expert opinion on the prevalence of identity theft, as the district court would have been helped if it had given consideration to the Plaintiff's witness on this point before giving summary judgment." (Andrews' expert witness was *Privacy Times* Publisher Evan Hendricks. While Judge Baird permitted him to testify about the scope of identity theft as it related to accuracy problems, she barred him from addressing the issue as it related to disclosure of credit reports.)

"The reasonableness of TRW's responses should also have been assessed by a jury with reference to the information TRW had indicating that the Imposter was not the Plaintiff. TRW argues that people do use nicknames and change addresses. But how many people misspell their first name? How many people mistake their date of birth? No rule of law answers these questions. A jury will have to say how reasonable a belief is that let an SSN trump all evidence of dissimilarity between the Plaintiff and the Imposter," Judge Noonan wrote.

The appeals court also rejected Judge Baird's finding that a decision favoring plaintiff would "impose too heavy a cost on TRW." Judge Noonan's response: "The FCRA has already made the determination as to what is a bearable cost for a credit reporting agency. The cost is what it takes to have a reasonable belief. In this case, that belief needed determination by a jury not a judge."

On the statute of limitations issue, the Ninth Circuit broke with view of several federal appeals courts that have concluded that they begin to toll when an FCRA violation occurs. Advocates have complained that many consumers don't learn of credit report problems until months, or even years, afterward.

"The general federal rule is that a federal statute of limitations begins to run when a party knows or has reason to know that she was injured. By this test, none of the Plaintiff's injuries were stale when suit was brought. . . . Neither the language of the statute nor its interpretation by other respected circuit courts of appeals is a warrant for disregarding the teaching of the Supreme Court: unless Congress has expressly legislated otherwise, the equitable doctrine of discovery 'is read into every federal statute of limitations,'" Judge Noonan wrote. (***Adelaide Andrews v. TRW, Inc.***: CA-9 -- No. 98-56624; July 17).

Furnisher Liability. Continuing a trend, a federal judge in Connecticut has ruled that the 1996 Amendments (Sect. 1681s-2) to the FCRA permit individuals to sue banks and other creditors who furnish inaccurate data to credit bureaus after they should have known better.

U.S. District Judge Janet Bond Arterton said that prior the 1996 Amendments, the FCRA limited the private right of action to credit bureaus and users of information. "By changing the language to 'any person,' which by its generality includes furnishers of information, Congress eliminated this information."

Last year, a federal court in Tennessee came to the opposite conclusion and barred a consumer from suing a bank that misreported data (***Carney v. Experian***, 57 F.Supp.2d 496, W.D. Tenn.) But Judge Atherton disagreed, noting that ***Carney*** Court made the ruling without a full hearing and after the plaintiff had failed to file an opposition. This year, she said, three courts have affirmed a private right of action against furnishers: ***Dornbecker v. Ameritech***, 2000 WL 758123, N.D. Illinois, June 8, 2000; ***DiMezza v. First USA Bank, Inc.***, 2000 WL 708458, New Mexico, May 1, 2000; and ***Campbell v. Baldwin***, 90 F.Supp.2d 754, E.D. Texas.

Judge Atherton said her view was supported by the FCRA's plain language, as well its legislative history and the Federal Trade Commission's rules. (***Henry McMillan v. Experian Information Systems***: USDC- Conn. -- No. 3:99cv1481)

WIRELESS: PHONE.COM, DOUBECLICK VOW PRIVACY IN LOCATION TRACKING

DoubleClick and Amazon.com are talking "opt-in." Not for the Internet, but for a future wave of advertising based on wireless technology's ability to track an individual's location.

On July 25, Silicon Valley's Phone.com announced plans and partnerships to develop "location-based" applications that also protect privacy by putting the individual in charge. With DoubleClick, Phone.com is developing a way to deliver ads based on the caller's whereabouts -- for instance, a consumer walking past a Gap store would be flashed Gap ads and sales.

Jamie Byrne, DoubleClick's director of "Emerging Platforms," said in a press release, "Phone.com sets an important precedent for the management of user privacy for the wireless Internet by requiring companies to request a consumer's permission before their location may be used. By giving consumers control of the usage of their data, of their data, the Mobile Location Server protects user privacy while providing carriers, wireless publishers and companies like DoubleClick with the tools to deliver highly targeted and relevant content, services and advertising. We look forward to working with Phone.com and privacy groups to ensure wireless advertising meets the standards of fair information practices."

With Amazon.com, it hopes to develop technology to enable shoppers to find the closest retailers or easiest online stores that sell products of interest. Ali Hussein, a director of Amazon Anywhere, said the arrangement would benefit Amazon's partners.

The basis for Phone.com's move is its new partnership with privately held SignalSoft, which provides network operators with emergency-911 solutions, zone-based billing, tracking and locations "translation" capability. The two firms plan to build a "Mobile Location Server" that will be available to wireless network operators "later this year," according to a press release.

Other partners include Go2Systems, which focuses on finding the nearest brick-and-mortar location, and In-Fusio, which specializes in location-based games, like a community treasure hunt.

Mark Hopper, Phone.com's senior product marketing manager, said, "Phone.com's location solution takes a leadership role in ensuring strong subscriber protection through privacy management, access controls, and other identity protecting capabilities, assuring end users that their location information is fully protected, " "Providing this kind of assurance enables wireless carriers and content providers to focus on business operations and brand management."

(*Privacy Times* left messages for both Hopper and Byrne, but they did not respond in time for our deadline.)

USAF PERSONNEL FILE DISCLOSED UNDER PRIVACY ACT NEED-TO-KNOW

A federal appeals panel in Washington ruled 2-1 that the Privacy Act's need-to-know exception justified a supervisor's review of the personnel file of an Air Force major who he suspected of misconduct.

Steven D.C. Bigelow, a major in the Information Warfare & Special Technical Operations Center, complained that neither the Privacy Act nor DOD regulations permitted his supervisor, Army Col. Nathan Noyes, to peruse his personnel file. Specifically, he said DOD rules do not instruct supervisors to search personnel files for derogatory information.

"We think this line of reasoning misses the point of the need-to-know exemption in the Privacy Act," wrote Judge XXX XX Randolph. "Sect. 552a(b)(1) does not require an agency to list those of its officers eligible to look at protected records, nor does it demand that an agency official be specifically assigned to examining records. What must be determined -- and what Judge Tatel (the dissenting judge) does not confront -- is whether the official examined the record in connection with the performance of duties assigned to him and whether he had to do so in order to perform those duties properly."

"Col. Noyes reviewed Maj. Bigelow's files in connection with his duty to make sure that the major was worthy of trust; and he had a need to examine the file in view of the doubts that had been raised in his mind about Bigelow and Bigelow's access to the country's top secrets."

In dissent, Judge Tatel said Noyes had a shared responsibility to assess Bigelow's trustworthiness, but not a right to examine his files. "The regulations protect the privacy of personnel security files by providing access only to certain specified officials (commanders and

security officer) and by requiring that supervisors like Noyes report their concerns to the Defense Investigative Service for further investigation." Judge Tatel noted that the Secretary of Defense had not included supervisors among those with "shared" responsibility who require access to personnel files. (***Steven Bidelow v. Dept. of Defense***: CA-D.C. -- No. 99-5280; July 14.)

FOIA CT. ROUNDUP: DOJ HIT FOR NOT INVOKING EXEMPTIONS

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

Keith Maydak v. U.S. Dept. of Justice: (No. 98-5492)

Court:	U.S. Court of Appeals for the District of Columbia
Judges:	Sentelle, Silberman & Rogers
Exemptions:	FOA (b)(7)(A), ongoing law enforcement investigations
Documents:	On Maydak, an inmate seeking to overturn conviction
Issue:	Does invoking only Ex. 7(A) permit agency to invoke other exemptions later?
Decided:	July 18, 2000

Rejecting the Justice Dept.'s bid for special treatment under Exemption 7(A), the appeals panel ruled that invoking Exemption 7(A) does not relieve an agency of its burden to invoke all relevant exemptions from the outset. In a move that must have stunned the government, it ordered the Justice Dept. to disclose all relevant records to inmate Keith Maydak. Ex. 7(A) protects records that, if disclosed, would interfere with ongoing law enforcement investigations.

"We conclude not only that the DOJ did not genuinely assert exemptions other than Exemption 7(A), but also that it had no legitimate excuse for its failure to do so," wrote Judge Sentelle. "There is simply nothing in the record to substantiate DOJ's claims that dire consequences will flow from the release of the requested documents."

"Furthermore, the DOJ's repeated statements that other specified FOIA exemptions might apply, coupled with its abject failure even to try to substantiate those assertions generically through affidavits, strongly suggests the sort of tactical maneuvering at a plaintiff's expense that we have explicitly rejected. If anything, the notions of judicial finality and economy, avoiding delay, and fairness dictate an order in Maydak's favor," he wrote.

Maydak remains incarcerated after being convicted in 1994 for mail and wire fraud and money laundering. When he filed his FOIA request, the Executive Office of U.S. Attorneys (EOUSA) initially invoked Exemption 7(A). But in 1996, the DOJ Office of Information and Privacy (OIP) remanded the case to EOUSA because Maydak's case was finished and Exemption 7(A) no longer applied.

Because Maydak continued appealing his conviction, EOUSA again invoked Ex. 7(A). Again, OIP remanded the case. In 1997, Maydak filed suit, and Ex. 7(A) was the only exemption invoked by the government.

DOJ argued that Ex. 7(A)'s unique protection for ongoing investigations creates a "blanket rule" allowing it to invoke other exemptions later if the government decides it is no longer applicable or a court rules against.

The appeals panel disagreed. "[FOIA] says nothing that would indicate that Ex. 7(A) is so unique," wrote Judge Sentelle. He rejected the DOJ's claim that it could not produce a *Vaughn* index for the other Exemptions because it would reveal what was protected by Ex. 7(A). Noting a high degree of flexibility in government affidavits in FOIA cases, Judge Sentelle said, "The government has mechanisms by which it can accomplish the goal of protecting sensitive information while at the same time satisfying its burden of proof with respect to other exemptions in the original district court proceedings."

IN OTHER CASES

Although finding the FBI's initial response "misleading," Judge Henry H. Kennedy, Jr. stayed a federal inmate's case until Oct. 1. "The Court cannot expect the agency to review an produce 11,000 pages of potentially responsive records overnight, particularly given its well-documented backlog," he wrote. (***Eric Burton v. FBI***: USDC-D.C. -- No. 99-2305; June 28.)

U.S. Magistrate Timothy Greeley has recommended dismissal of a case brought by a man who accused the FBI of disrupting his life. "For example, [the FBI] caused emergency personnel to drive fire trucks and ambulances in cities and towns that plaintiff resided in or drove through, and caused Canadian and U.S. border crossing agents to harass him on several occasions while entering or exiting Canada, and spoke with individuals of the general public about plaintiff to find out information and harm his reputation," wrote Judge Greeley, who called allegations "delusional, irrational and wholly incredible." However, the FBI disclosed 133 pages to the plaintiff. (***Michael John Twomey v. FBI***: USDC-W.D. Mich. (North) -- No. 99-041; July 14.)

IN BRIEF . . .

In the state's first class-action suit against companies that send unsolicited faxes, the Court of Appeals of Georgia has given the green light to a class action suit against the restaurant chain Hooters. A sole practitioner attorney brought the case against the Augusta, Ga., restaurant chain. The case establishes the precedent that a federal statute regulating faxed ads and other telemarketing efforts creates a private right of action and confers jurisdiction on state courts in Georgia. (***Hooters of Augusta Inc. v. Nicholson*** No. A00A0429 (Ct. App. Ga. July 14)

Law Firm Payroll Data

A New York State appeals court has ruled that former partners of a law firm are liable for distributing information about the salaries of associates and support staff when still at the firm. The 3-2 ruling in *Gibbs v. Breed Abbott & Morgan, 3040-3041* dealt mainly with the fiduciary responsibilities of attorneys who leave their firm and take correspondence and other materials and assets with them.

Financial Privacy Conference

A conference on financial privacy will be held in New York City's The Regency on September 7-8. The parley features leading attorneys including Hugh Jewett, First Data vice president, Michael Hogan, general counsel of DLJ Direct, Richard McLaughlin, V.P., Royal Bank of Canada, W. Scott Blackmere, attorney, Deborah Thoren-Peden, general counsel & CPO of PayMyBills.com, and Margaret Paradis, senior associate general counsel of PaineWebber. The event is sponsored by ICM. Cost: $2,400. Contact: yaelk@finstrany.com; One Exchange Plaza, 55 Broadway, 26th Fl., NY, NY; (212) 363-8200 x 277; (212) 363-7714 [fax].

YES I Want To Subscribe & Save 20% Off The $310 Annual Rate

_____ $250 Per Year (23 Issues)
_____ $455 2-Year (46 issues)

_____
Credit Card No. (Visa, MC or Amex)

_____ Expiration Date

(Or you can pay by Check or Purchase Order)

Name _____
Org. _____
Address _____
City/ST/ZIP _____

Phone No. _____

Privacy Times
P.O. Box 21501
Washington, D.C. 20009
(202) 829-3660 [Ph] 829-3653 [fax]

evan@privacytimes.com — www.privacytimes.com