What Else Should be Keeping You Up at Night – Current Uses and Abuses of the Internet

March 31, 2009
Los Angeles, CA

ALSTON+BIRD LLP

What Should I Be Doing About Data Security and Privacy Right Now?

- **A Panel Discussion: Issues and Scenarios**

Jon Gordon, Alston + Bird, LLP, Moderator

Tom Arbogast, BT, VP and Director Commercial Collaboration for BT Design

Todd McClelland, Alston + Bird, LLP

Mike Zweiback, Alston + Bird, LLP

ALSTON+BIRD LLP

What Should I Be Doing About Data Security and Privacy Right Now?

Tom Arbogast, BT Design

Tom is Vice President and Director of Commercial Collaboration for BT Design, BT's IT arm, comprised of nearly 20,000 global employees. He handles major IT supplier, customer and outsourcing negotiations and oversees the implementation of large IT projects from a commercial perspective. Prior to joining BT, he served as an Executive Vice President for a small telco and also worked in a business development/commercial-legal capacity for a large professional services consulting company. He previously worked as appellate counsel in Canada and has argued numerous cases before the Supreme Court of Canada and the BC Court of Appeal.

Todd McClelland, Alston & Bird, LLP

Todd McClelland specializes in strategic corporate projects that include significant technology, IP, outsourcing, or energy components. His practice scope includes IT systems procurement and infrastructure, outsourcing projects, energy policy, construction projects, intellectual property management, business model innovation activities and technology and energy company representation. In addition to his transactional practice, Todd is a registered patent attorney and provides counsel on patent licensing, avoidance and procurement.

Michael Zweiback, Alston & Bird, LLP

Michael Zweiback is a partner in the firm's Los Angeles office focusing his practice on governmental and corporate investigations, white collar criminal defense, environmental crimes, privacy and data security matters. He joins the firm from the U.S. Attorney's Office in Los Angeles, where he had been chief of the Cyber and Intellectual Property Crimes Section since 2007.

Jonathan Gordon, Alston & Bird, LLP

Jonathan Gordon, partner in the firm's Los Angeles office, advises clients involved in the commercialization of new technologies, intellectual property and licensing transactions, and technology research and development. He counsels clients on their business transactions and practices over the Internet. Mr. Gordon also handles disputes involving licenses, patents, copyrights, trademarks and trade secrets, as well as other business disputes. He has represented clients in state and federal courts and in a variety of domestic and international arbitration forums.

ALSTON+BIRD LLP

What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario #1: Laptops– Should we lock them back into their docking stations?**

  Company employees globe-trotting and vacationing with their laptops containing PII (personally identifiable information) and Company trade secrets: What do you do when the laptop is stolen, hacked or searched at a border? What measures should you be taking now?

ALSTON+BIRD LLP

What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario # 2: Printed medical and personal data in the dumpster– the FTC case against CVS.**

  CVS Caremark stores were alleged to have regularly put in dumpters pill containers and documents containing personal medical information, social security numbers, payroll information, insurance cards, account numbers, driver's license numbers and HIPAA-protected information. Multi-faceted remedies enforced by FTC, including 20 years of audits and $2.25MM payment.

What Should I Be Doing About Data Security and Privacy Right Now?

DATAFLOW Analysis and Software Development Lifecycle

- The traditional "CIA" model for analyzing information in a data/IT context addresses: Confidentiality / Integrity / Availability
- From a project, or ground-up perspective, this can be viewed as:
- Concurrency / Iteration / Accessibility
- It is important to understand the stages of the Software Development Lifecycle. This will in turn lead to an understanding of DATAFLOW

What Should I Be Doing About Data Security and Privacy Right Now?

DATAFLOW Chart Considerations:

- Creation and Collection
- Storage and Handling (Classification)
- Migration and Transit (and accessibility in context)
- Conversion and Use
- Restrictions (Legal, Regulatory, Policy and Business)
- Retention and Destruction Requirements
- Authorization and Administration Policy

ALSTON+BIRD LLP

What Should I Be Doing About Data Security and Privacy Right Now?

Agile Development and Iterative Cycles for DATAFLOW Analysis

- Requirements Analysis
- Design and Build
- Implement
- Test
- These steps are becoming iterative and repeatable and require concurrent input from Legal/Regulatory to properly monitor privacy and security issues

ALSTON+BIRD LLP

What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario #3: What responsibility do you have for third parties who have access to your systems or data?**

  A mortgage lender in Texas allowed its database to be accessed by a third party home-seller. Third party was then hacked and lender's database was compromised allowing access to credit reports and personal financial information of lender's customers. FTC imposes comprehensive remedies including 20 year requirements.

What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario #4: No breach ≠ no enforcement**

  London stockbroker had "casual" practices regarding customer personal and financial information over phone calls, published in unsecured mailings, and stored as unencrypted data at employees' homes. There was no known breach or theft of this data. FSA (UK Financial Services Authority) enforces fine and remedies.

What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario #5: Heartburn at Heartland**

100 million credit card records compromised when a weak point in the company's data flow process is attacked and un-encrypted data is accessed. What are the costs of security incidents?

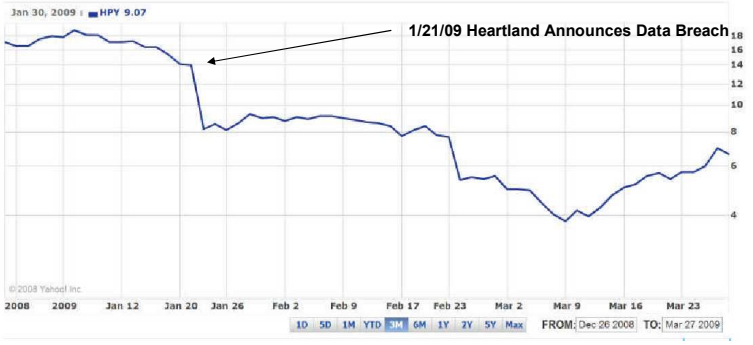
What Should I Be Doing About Data Security and Privacy Right Now?

YAHOO! FINANCE **Heartland Payment Systems Inc. (HPY)**

7.02	Open:	6.27	Mkt Cap:	262.84M	P/E:	6.49	Dividend:	0.03
+1.01 (16.81%)	High:	7.18	52Wk High:	33.00	F P/E:	-	Yield:	1.42
Mar 26 - Close	Low:	6.19	52Wk Low:	3.57	Beta:	1.47	Shares:	37.44M
	Vol:	908,223.00	Avg Vol:	738,000.00	EPS:	1.08	Inst. Own:	74%

After Hours: 7.02 0.00 (0.00%) - Mar 26, 5:01PM EDT

NYSE Real-time data - Disclaimer



What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario #6: A "logic bomb" at Fannie Mae and the hazards of the "hack back."**

  A trusted employee/contractor is being terminated and, on the way out the door, he plants a logic bomb into the company's server that will literally destroy all data on 4,000 company servers. Miraculously discovered "by accident, " detonation of the bomb was averted.

What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario #7: Cloud computing– the wave of the future has a tsunami of data security issues**

  Everyone is singing the praises of "the cloud" to cut costs and enable applications. But, is the cloud secure? How do you monitor and control your risks? Who are you dealing with, where is the infrastructure and who is accountable?

What Should I Be Doing About Data Security and Privacy Right Now?

- **Scenario # 8: New state enforcement schemes everywhere you turn– how do you manage this?**

  New state legislation is coming fast and furious from many jurisdictions (e.g., California, Massachusetts, New York, Nevada, Connecticut, Texas, New Jersey), layered on top of the FTC, and HIPAA regimes, not to mention the EU Data Directive and global regulation. How do you respond and manage this and what does the future hold?

Supporting Materials

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellant,* v. MICHAEL TIMOTHY ARNOLD, *Defendant-Appellee.*	No. 06-50581 D.C. No. CR-05-00772-DDP ORDER AND AMENDED OPINION

Appeal from the United States District Court
for the Central District of California
Dean D. Pregerson, District Judge, Presiding

Argued and Submitted
October 18, 2007—Pasadena, California

Filed April 21, 2008
Amended July 10, 2008

Before: Diarmuid F. O'Scannlain and Milan D. Smith, Jr.,
Circuit Judges, and Michael W. Mosman,* District Judge.

Opinion by Judge O'Scannlain

*The Honorable Michael W. Mosman, United States District Judge for the District of Oregon, sitting by designation.

COUNSEL

Steve Kim, Assistant United States Attorney, Criminal Appeals Section, Los Angeles, California, argued the cause for the plaintiff-appellant and filed briefs; George S. Cardona, United States Attorney, and Thomas P. O'Brien, Assistant United States Attorney, Chief, Criminal Division, Los Angeles, California, were on the briefs.

Marilyn E. Bednarski, Kaye, McLane, & Bednarski, LLP, Pasadena, California, argued the cause for the defendant-appellee and filed a brief; Kevin Lahue, Kaye, McLane, & Bednarski, LLP, Pasadena, California, was on the brief.

ORDER

The opinion filed April 21, 2008, is amended as follows:

1. At 523 F.3d 941, 946 n.1 (9th Cir. 2008), in the first sentence replace "incoming" with "outgoing."

With the foregoing amendment, the panel has unanimously voted to deny the petition for rehearing. Judge O'Scannlain and Judge M. Smith, Jr., vote to deny the petition for rehearing en banc and Judge Mosman so recommends. The full court has been advised of the petition for rehearing en banc and no active judge has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 35.

The petition for rehearing and the petition for rehearing en banc are DENIED. Further petitions for rehearing or rehearing en banc may not be filed.

OPINION

O'SCANNLAIN, Circuit Judge:

We must decide whether customs officers at Los Angeles International Airport may examine the electronic contents of a passenger's laptop computer without reasonable suspicion.

I

On July 17, 2005, forty-three-year-old Michael Arnold arrived at Los Angeles International Airport ("LAX") after a nearly twenty-hour flight from the Philippines. After retrieving his luggage from the baggage claim, Arnold proceeded to customs. U.S. Customs and Border Patrol ("CBP") Officer Laura Peng first saw Arnold while he was in line waiting to go through the checkpoint and selected him for secondary questioning. She asked Arnold where he had traveled, the purpose of his travel, and the length of his trip. Arnold stated that he had been on vacation for three weeks visiting friends in the Philippines.

Peng then inspected Arnold's luggage, which contained his laptop computer, a separate hard drive, a computer memory stick (also called a flash drive or USB drive), and six compact discs. Peng instructed Arnold to turn on the computer so she could see if it was functioning. While the computer was booting up, Peng turned it over to her colleague, CBP Officer John Roberts, and continued to inspect Arnold's luggage.

When the computer had booted up, its desktop displayed numerous icons and folders. Two folders were entitled "Kodak Pictures" and one was entitled "Kodak Memories." Peng and Roberts clicked on the Kodak folders, opened the files, and viewed the photos on Arnold's computer including one that depicted two nude women. Roberts called in supervisors, who in turn called in special agents with the United States Department of Homeland Security, Immigration and

Customs Enforcement ("ICE"). The ICE agents questioned Arnold about the contents of his computer and detained him for several hours. They examined the computer equipment and found numerous images depicting what they believed to be child pornography. The officers seized the computer and storage devices but released Arnold. Two weeks later, federal agents obtained a warrant.

A grand jury charged Arnold with: (1) "knowingly transport[ing] child pornography, as defined in [18 U.S.C. § 2256(8)(A)], in interstate and foreign commerce, by any means, including by computer, knowing that the images were child pornography"; (2) "knowingly possess[ing] a computer hard drive and compact discs which both contained more than one image of child pornography, as defined in [18 U.S.C. § 2256(8)(A)], that had been shipped and transported in interstate and foreign commerce by any means, including by computer, knowing that the images were child pornography"; and (3) "knowingly and intentionally travel[ing] in foreign commerce and attempt[ing] to engage in illicit sexual conduct, as defined in [18 U.S.C. § 2423(f)], in a foreign place, namely, the Philippines, with a person under 18 years of age, in violation of [18 U.S.C. § 2423(c)]."

Arnold filed a motion to suppress arguing that the government conducted the search without reasonable suspicion. The government countered that: (1) reasonable suspicion was not required under the Fourth Amendment because of the border-search doctrine; and (2) if reasonable suspicion were necessary, that it was present in this case.

The district court granted Arnold's motion to suppress finding that: (1) reasonable suspicion was indeed necessary to search the laptop; and (2) the government had failed to meet the burden of showing that the CBP officers had reasonable suspicion to search.

The government timely appealed the district court's order granting the motion to suppress.

II

Arnold argues that the district court was correct in concluding that reasonable suspicion was required to search his laptop at the border because it is distinguishable from other containers of documents based on its ability to store greater amounts of information and its unique role in modern life.

Arnold argues that "laptop computers are fundamentally different from traditional closed containers," and analogizes them to "homes" and the "human mind." Arnold's analogy of a laptop to a home is based on his conclusion that a laptop's capacity allows for the storage of personal documents in an amount equivalent to that stored in one's home. He argues that a laptop is like the "human mind" because of its ability to record ideas, e-mail, internet chats and web-surfing habits.

Lastly, Arnold argues that application of First Amendment principles requires us to rule contrary to the Fourth Circuit in *United States v. Ickes*, 393 F.3d 501, 506-08 (4th Cir. 2005) (rejecting the argument based on the First Amendment that a higher level of suspicion is needed for searches of "expressive material"), and to promulgate a reasonable suspicion requirement for border searches where the risk is high that expressive material will be exposed.

III

A

[1] The Fourth Amendment states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. Const. amend. IV. Searches of international passengers at American airports are considered border searches because they occur at the "functional equivalent of a border." *Almeida-Sanchez v. United States*, 413 U.S. 266, 273 (1973) ("For . . . example, a search of the passengers and

cargo of an airplane arriving at a St. Louis airport after a non-stop flight from Mexico City would clearly be the functional equivalent of a border search."). "It is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). Generally, "searches made at the border . . . are reasonable simply by virtue of the fact that they occur at the border . . . ." *United States v. Ramsey*, 431 U.S. 606, 616 (1977).

[2] The Supreme Court has stated that:

> The authority of the United States to search the baggage of arriving international travelers is based on its inherent sovereign authority to protect its territorial integrity. By reason of that authority, it is entitled to require that whoever seeks entry must establish the right to enter and to bring into the country whatever he may carry.

Torres v. Puerto Rico, 442 U.S. 465, 472-73 (1979). In other words, the "Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *Flores-Montano*, 541 U.S. at 152. Therefore, "[t]he luggage carried by a traveler entering the country may be searched at random by a customs officer . . . no matter how great the traveler's desire to conceal the contents may be." *United States v. Ross*, 456 U.S. 798, 823 (1982). Furthermore, "a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf [may] claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case." *Id.* at 822.

B

[3] Courts have long held that searches of closed containers and their contents can be conducted at the border without par-

ticularized suspicion under the Fourth Amendment. Searches of the following specific items have been upheld without particularized suspicion: (1) the contents of a traveler's briefcase and luggage, *United States v. Tsai*, 282 F.3d 690, 696 (9th Cir. 2002); (2) a traveler's "purse, wallet, or pockets," *Henderson v. United States*, 390 F.2d 805, 808 (9th Cir. 1967); (3) papers found in containers such as pockets, see *United States v. Grayson*, 597 F.2d 1225, 1228-29 (9th Cir. 1979) (allowing search without particularized suspicion of papers found in a shirt pocket); and (4) pictures, films and other graphic materials. *See United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971); *see also 12,200-Ft. Reels of Super 8MM. Film*, 413 U.S. 123, 124-25 (1973) ("Import restrictions and searches of persons or packages at the national borders rest on different considerations and different rules of constitutional law from domestic regulations.").

Nevertheless, the Supreme Court has drawn some limits on the border search power. Specifically, the Supreme Court has held that reasonable suspicion is required to search a traveler's "alimentary canal," *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985), because " '[t]he interests in human dignity and privacy which the Fourth Amendment protects forbid any such intrusion [beyond the body's surface] on the mere chance that desired evidence might be obtained.' " *Id.* at 540 n.3 (quoting *Schmerber v. California*, 384 U.S. 757, 769 (1966)). However, it has expressly declined to decide "what level of suspicion, *if any*, is required for nonroutine border searches such as strip, body cavity, or involuntary x-ray searches." *Id.* at 541 n.4 (emphasis added). Furthermore, the Supreme Court has rejected creating a balancing test based on a "routine" and "nonroutine" search framework, and has treated the terms as purely descriptive. *See United States v. Cortez-Rocha*, 394 F.3d 1115, 1122 (9th Cir. 2005).

[4] Other than when "intrusive searches of *the person*" are at issue, *Flores-Montano*, 541 U.S. at 152 (emphasis added),

the Supreme Court has held open the possibility, "that some searches of *property* are so destructive as to require" particularized suspicion. *Id.* at 155-56 (emphasis added) (holding that complete disassembly and reassembly of a car gas tank did not require particularized suspicion). Indeed, the Supreme Court has left open the question of " 'whether, and under what circumstances, a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out.' " *Id.* at 155 n.2 (quoting *Ramsey*, 431 U.S. at 618 n.13).

C

In any event, the district court's holding that particularized suspicion is required to search a laptop, based on cases involving the search of the person, was erroneous. Its reliance on such cases as *United States v. Vance*, 62 F.3d 1152, 1156 (9th Cir. 1995) (holding that "[a]s the search becomes more intrusive, more suspicion is needed" in the context of a search of the human body), to support its use of a sliding intrusiveness scale to determine when reasonable suspicion is needed to search property at the border is misplaced. *United States v. Arnold*, 454 F. Supp. 2d 999, 1002-04 (C.D. Cal. 2006).

[5] The Supreme Court has stated that "[c]omplex balancing tests to determine what is a 'routine' search of a vehicle, as opposed to a more 'intrusive' search of a person, have no place in border searches of vehicles." *Flores-Montano*, 541 U.S. at 152. Arnold argues that the district court was correct to apply an intrusiveness analysis to a laptop search despite the Supreme Court's holding in *Flores-Montano*, by distinguishing between one's privacy interest in a vehicle compared to a laptop. However, this attempt to distinguish *Flores-Montano* is off the mark. The Supreme Court's analysis determining what protection to give a vehicle was not based on the unique characteristics of vehicles with respect to other property, but was based on the fact that a vehicle, as a piece of property, simply does not implicate the same "dignity and pri-

vacy" concerns as "highly intrusive searches of the person." *Flores-Montano*, 541 U.S. at 152.

[6] Furthermore, we have expressly repudiated this type of "least restrictive means test" in the border search context. *See Cortez-Rocha*, 394 F.3d at 1123 (refusing to fashion a "least restrictive means test for border control vehicular searches, and . . . refus[ing] to tie the hands of border control inspectors in such a fashion"). Moreover, in both *United States v. Chaudhry*, 424 F.3d 1051, 1054 (9th Cir. 2005) (finding the distinction between "routine" and "non-routine" inapplicable to searches of property) and *Cortez-Rocha*, 394 F.3d at 1122-23, we have recognized that *Flores-Montano* rejected our prior approach of using an intrusiveness analysis to determine the reasonableness of property searches at the international border.

[7] Therefore, we are satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border.[1]

IV

While the Supreme Court left open the possibility of requiring reasonable suspicion for certain border searches of property in *Flores-Montano*, 541 U.S. at 155-56, the district court did not base its holding on the two narrow grounds left open by the Supreme Court in that case.

Arnold has never claimed that the government's search of his laptop damaged it in any way; therefore, we need not con-

[1]We recently issued an opinion on a separate issue of whether reasonable suspicion is required to search outgoing international correspondence; however, this opinion has since been withdrawn and the case has been reheard by an en banc panel of this court that has yet to issue a decision. *United States v. Seljan*, 497 F.3d 1035 (9th Cir. 2007), *withdrawn by* 512 F.3d 1203 (9th Cir. 2008) (ordering rehearing en banc).

sider whether "exceptional damage to property" applies. Arnold does raise the "particularly offensive manner" exception to the government's broad border search powers.[2] But, there is nothing in the record to indicate that the manner in which the CBP officers conducted the search was "particularly offensive" in comparison with other lawful border searches. According to Arnold, the CBP officers simply "had me boot [the laptop] up, and looked at what I had inside . . . ."

[8] Whatever "particularly offensive manner" might mean, this search certainly does not meet that test. Arnold has failed to distinguish how the search of his laptop and its electronic contents is logically any different from the suspicionless border searches of travelers' luggage that the Supreme Court and we have allowed. *See Ross*, 456 U.S. at 823; *see also Vance*, 62 F.3d at 1156 ("In a border search, a person is subject to search of luggage, contents of pockets and purse without any suspicion at all.").

[9] With respect to these searches, the Supreme Court has refused to draw distinctions between containers of information and contraband with respect to their quality or nature for purposes of determining the appropriate level of Fourth Amendment protection. Arnold's analogy to a search of a home based on a laptop's storage capacity is without merit. The Supreme Court has expressly rejected applying the

[2]Notwithstanding the government's objection, we can decide this issue because the "particularly offensive manner" exception can be found in *Flores-Montano*, which was presented to the district court by the parties, and "the matter [of what the Fourth Amendment requires] was fairly before the [district court]" and, in any event, it is a question of law. *See Nelson v. Adams USA, Inc.*, 529 U.S. 460, 469-70 (2000); *see also Ballaris v. Wacker Siltronic Corp.*, 370 F.3d 901, 908 (9th Cir. 2004) ("Once a federal claim is properly presented, a party can make any argument in support of that claim; parties are not limited to the precise argument they made below. . . . Where . . . the question presented is one of law, we consider it in light of all relevant authority, regardless of whether such authority was properly presented in the district court." (citations and quotation marks omitted)).

Fourth Amendment protections afforded to homes to property which is "*capable of functioning as a home*" simply due to its size, or, distinguishing between " 'worthy and 'unworthy' containers." *California v. Carney*, 471 U.S. 386, 393-94 (1985).

In *Carney*, the Supreme Court rejected the argument that evidence obtained from a warrantless search of a mobile home should be suppressed because it was "*capable of functioning as a home*." *Id*. at 387-88, 393-94. The Supreme Court refused to treat a mobile home differently from other vehicles just because it could be used as a home. *Id.* at 394-95. The two main reasons that the Court gave in support of its holding, were: (1) that a mobile home is "readily movable," and (2) that "the expectation [of privacy] with respect to one's automobile is significantly less than that relating to one's home or office." *Id.* at 391 (quotation marks omitted).

[10] Here, beyond the simple fact that one cannot live in a laptop, *Carney* militates against the proposition that a laptop is a home. First, as Arnold himself admits, a laptop goes with the person, and, therefore is "readily mobile." *Carney*, 471 U.S. at 391. Second, one's "expectation of privacy [at the border] . . . is significantly less than that relating to one's home or office." *Id.*

Moreover, case law does not support a finding that a search which occurs in an otherwise ordinary manner, is "particularly offensive" simply due to the storage capacity of the object being searched. *See California v. Acevedo*, 500 U.S. 565, 576 (1991) (refusing to find that "looking inside a closed container" when already properly searching a car was unreasonable when the Court had previously found "destroying the interior of an automobile" to be reasonable in *Carroll v. United States*, 267 U.S. 132 (1925)).

[11] Because there is no basis in the record to support the contention that the manner in which the search occurred was

"particularly offensive" in light of other searches allowed by the Supreme Court and our precedents, the district court's judgment cannot be sustained.

V

Finally, despite Arnold's arguments to the contrary we are unpersuaded that we should create a split with the Fourth Circuit's decision in *Ickes*. In that case, the defendant was stopped by Customs agents as he attempted to drive his van from Canada into the United States. 393 F.3d at 502. Upon a "cursory search" of defendant's van, the inspecting agent discovered a video camera containing a tape of a tennis match which "focused excessively on a young ball boy." *Id*. This prompted a more thorough examination of the vehicle, which uncovered several photograph albums depicting provocatively-posed prepubescent boys, most nude or semi-nude. *Id.* at 503.

The Fourth Circuit held that the warrantless search of defendant's van was permissible under the border search doctrine. The court refused to carve out a First Amendment exception to that doctrine because such a rule would: (1) protect terrorist communications "which are inherently 'expressive' "; (2) create an unworkable standard for government agents who "would have to decide—on their feet—which expressive material is covered by the First Amendment"; and (3) contravene the weight of Supreme Court precedent refusing to subject government action to greater scrutiny with respect to the Fourth Amendment when an alleged First Amendment interest is also at stake. *See id.* at 506-08 (citing *New York v. P.J. Video*, 475 U.S. 868, 874 (1986) (refusing to require a higher standard of probable cause for warrant applications when expressive material is involved)).

We are persuaded by the analysis of our sister circuit and will follow the reasoning of *Ickes* in this case.

VI

For the foregoing reasons, the district court's decision to grant Arnold's motion to suppress must be

REVERSED.

Taking your laptop into the US? Be sure to hide all your data first

Bruce Schneier

The Guardian, Thursday 15 May 2008

http://www.guardian.co.uk/technology/2008/may/15/computing.security

Stolen Laptop Helps Turn Tables on Suspects

By LISA W. FODERARO
Published: May 10, 2008

http://www.nytimes.com/2008/05/10/nyregion/10laptop.html?_r=1&oref=slogin

$20 Million Settlement Reached for Veterans in ID Theft Suit

By THE ASSOCIATED PRESS
Published: January 27, 2009

http://www.nytimes.com/2009/01/28/washington/28vets.html

For Release: February 18, 2009

CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations

MEDIA CONTACT:

Claudia Bourne Farrell,
Office of Public Affairs
202-326-2181

STAFF CONTACT:

Alain Sheer,
Bureau of Consumer Protection
202-326-2252

Loretta Garrison,
Bureau of Consumer Protection
202-326-2252

(FTC File No. 072 3119)
(cvs)

http://www.ftc.gov/opa/2009/02/cvs.shtm

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of
CVS CAREMARK CORPORATION, a corporation,

Complaint

http://www.ftc.gov/os/caselist/0723119/090218cvscmpt.pdf

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of
CVS CAREMARK CORPORATION, a corporation,

Complaint: Exhibit A

http://www.ftc.gov/os/caselist/0723119/090218cvscmptexha.pdf

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of
CVS CAREMARK CORPORATION, a corporation,

AGREEMENT CONTAINING CONSENT ORDER

http://www.ftc.gov/os/caselist/0723119/090218cvsagree.pdf

Analysis of Proposed Consent Order to Aid Public Comment

In the Matter of CVS Caremark Corporation, File No. 0723119

http://www.ftc.gov/os/caselist/0723119/090218cvsanal.pdf

For Release: November 6, 2008

Mortgage Company Settles Data Security Charges

Data Breach Compromised Privacy of Hundreds of Consumers

MEDIA CONTACT:

Betsy Lordan,
Office of Public Affairs
202-326-3707

STAFF CONTACT:

Jessica Rich,
Bureau of Consumer Protection
202-326-2148

(FTC File No. 0723004)
(PCL.final.wpd)

http://www.ftc.gov/opa/2008/11/pcl.shtm

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of PREMIER CAPITAL LENDING, INC. a corporation; and DEBRA STILES, individually and as an officer of the corporation.

Complaint

http://www.ftc.gov/os/caselist/0723004/081206pclcmpt.pdf

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of PREMIER CAPITAL LENDING, INC. a corporation; and DEBRA STILES, individually and as an officer of the corporation.

Decision and Order

http://www.ftc.gov/os/caselist/0723004/081216pcldo.pdf

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of PREMIER CAPITAL LENDING, INC. a corporation; and DEBRA STILES, individually and as an officer of the corporation.

Agreement Containing Consent Order

http://www.ftc.gov/os/caselist/0723004/081106pclagree.pdf

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of PREMIER CAPITAL LENDING, INC. a corporation; and DEBRA STILES, individually and as an officer of the corporation.

Analysis of Proposed Consent Order to Aid Public Comment

http://www.ftc.gov/os/caselist/0723004/081106pclagree.pdf

FSA fines stockbroker Merchant Securities for slack security

18 June 2008 - 10:10

http://www.finextra.com/fullstory.asp?id=18599

London FSA Matter

13 June 2008

Summary: The Financial Services Authority of 25 The North Colonnade, Canary Wharf, London E14 5HS (the FSA) gives you final notice about a requirement to pay a financial penalty.

http://www.fsa.gov.uk/pubs/final/merchant_13jun08.pdf

Stockbroking firm fined £77,000 for weak Data Security Controls

17 June 2008

http://www.fsa.gov.uk/pages/Library/Communication/PR/2008/058.shtml

Cost of a Security Breach

Friday, April 13, 2007

http://securityspace.blogspot.com/2007/04/cost-of-security-breach.html

The Real Cost of a Security Breach

David Hobson, Managing Director of Global Gecure Systems

August 12, 2008

http://www.scmagazineus.com/The-real-cost-of-a-security-breach/article/113717/

Security 101: Cost of a Breach

http://www.secureworks.com/research/newsletter/2007/10/

Fannie Mae Logic Bomb Would Have Caused Weeklong Shutdown

By Kevin Poulsen | January 29, 2009 | 1:41:19 PM | Categories: Threats

http://blog.wired.com/27bstroke6/2009/01/fannie.html

Fannie Mae Logic Bomb Makes Case For Strong IDM

Posted by: **George Hulme, Jan 29, 2009 09:27 PM**

http://www.informationweek.com/blog/main/archives/2009/01/fannie_mae_logi.html

FTC questions cloud-computing security

By Stephanie Condon
March 17, 2009 6:30 PM PDT

http://news.cnet.com/8301-13578_3-10198577-38.html

Privacy & Security Task Force ADVISORY

States Adopting Aggressive New Privacy and Data Security Laws and Regulations

October 7, 2008

http://www.alston.com/files/Publication/05c1737d-ccfc-44a2-9252-1ffbea8953d3/Presentation/PublicationAttachment/a5a0be6c-e8c5-4b3c-ad17-134c3b6f0cd6/Privacy%20Post%20Vol%204.pdf

If you would like to receive future *Privacy & Security Task Force Advisories* electronically, please forward your contact information including e-mail address to **Privacy.Post@alston.com.** Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information please contact your Alston & Bird attorney or any of our **Privacy & Security Task Force** attorneys.

201 CMR 17.00:
Standards for The Protection of Personal Information of Residents of the Commonwealth

http://www.mass.gov/?pageID=ocaterminal&L=4&L0=Home&L1=Consumer&L2=Privacy&L3=Identity+Theft&sid=Eoca&b=terminalcontent&f=reg201cmr17&csid=Eoca

SB 20 Senate Bill Analysis
Senate Judiciary Commitee
Senator Ellen M. Corbett, Chair
2009-2010 Regular Session

http://info.sen.ca.gov/pub/09-10/bill/sen/sb_0001-0050/sb_20_cfa_20090224_164247_sen_comm.html

AMENDED IN SENATE MARCH 4, 2009

SENATE BILL No. 20

Introduced by Senator Simitian

December 1, 2008

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 20, as amended, Simitian. Personal information: privacy.

Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the system or data, as defined, following discovery or notification of the security breach, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

This bill would require any agency, person, or business that must issue a security breach notification pursuant to existing law to fulfill certain additional requirements pertaining to the security breach notification, as specified.

The bill would also require any agency, person, or business that must issue a security breach notification to more than 500 California residents pursuant to existing law to electronically submit that security breach notification to the Attorney General.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 1798.29 of the Civil Code is amended to read:

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that must issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information~~, as defined in subdivision (g),~~ that were or are reasonably believed to have been the subject of a breach.

(C) The date, estimated date, or date range within which the breach occurred, if that information is possible to determine at the time the notice is provided, and the date of the notice.

(D) Whether the notification was delayed as a result of a law enforcement investigation.

(E) A general description of the breach incident.

(F) The estimated number of persons affected by the breach.

(G) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a bank account or credit card number, a social security number, or a driver's license or California identification card number.

(3) At the discretion of the agency, the security breach notification may also include any of the following:

(A) Information about what the agency has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) Any agency that must issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit that security breach notification to the Attorney General.

(f) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(g) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(4) Medical information.

(5) Health insurance information.

(h) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully

made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(i) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.

(C) Notification to major statewide media and the Office of Information Security and Privacy Protection.

(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 2. Section 1798.82 of the Civil Code is amended to read:

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the

security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any person or business that must issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information~~, as defined in subdivision (g),~~ that were or are reasonably believed to have been the subject of a breach.

(C) The date, or estimated date, or date range within which the breach occurred, if that information is possible to determine at the time the notice is provided, and the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation.

(E) A general description of the breach incident.

(F) The estimated number of persons affected by the breach.

(G) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a bank account or credit card number, a social security number, or a driver's license or California identification card number.

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) Any person or business that must issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit that security breach notification to the Attorney General.

(f) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(g) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(4) Medical information.

(5) Health insurance information.

(h) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(i) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media and the Office of Information Security and Privacy Protection.

(j) Notwithstanding subdivision (i), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

O

Annotated Internet Links: Global Data Security and Privacy

http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:EN:PDF
December 27, 2001, European Commission Decision with recommended clauses for transfer of data to third parties outside of the EEA ("European Economic Area" including EU member countries and other countries implementing the Directive of October 24, 1995).

http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
European Commission home page for data protection resources.

http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm
European Commission list of European, US, and Asian Data Protection Commissioners and privacy officers.

http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm
European Commission page with multiple resources relating to model contracts for transfer of data to non-EU countries.

http://useu.usmission.gov/Dossiers/Data_Privacy/default.asp
Main Data Privacy page of the US Mission to the European Union.

http://useu.usmission.gov/Dossiers/Data_Privacy/Dec1208_SLCG_Statement.asp\
December 12, 2008, US, EU Issue Statement on Common Data Privacy and Protection Principles (focused on anti-terrorism and law enforcement issues)

http://ftc.gov/privacy/
FTC Main page for privacy initiatives, including news of enforcement actions, and information on deception (misleading consumers re privacy practices), financial privacy, credit reporting and children's privacy.

http://www.ftc.gov/infosecurity/
FTC interactive guide for businesses on protecting personal information.

http://www.export.gov/safeharbor/
US Department of Commerce site on "Safe Harbor" for data protection/privacy transactions with European countries.

http://www.export.gov/safeharbor/SH_Overview.asp
Safe Harbor Overview including list of key Safe Harbor principles

http://www.export.gov/safeharbor/Sh_Checklist.asp
Safe Harbor checklist

http://www.export.gov/safeharbor/SH_Documents.asp
Comprehensive set of Safe Harbor documents (including critical FAQs)

http://export.gov/safeharbor/SH_Helpful_Hints.asp
Helpful Hints for a Safe Harbor policy and compliance

http://export.gov/safeharbor/SH_Privacy_Links.asp
Data Privacy links and further resources

http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list
US Department of Commerce list of organizations representing that they have complied with safe harbor policy framework.

http://infotech.aicpa.org/Resources/Systems+Audit+and+Internal+Control/IT+Systems+Audit/Standards+and+Regulations/SAS+No.+70+Service+Organizations.htm
AICPA resource page for auditors' guidelines on SAS 70

http://infotech.aicpa.org/Resources/Privacy/
AICPA privacy resource page (note that beta "privacy tool" is available only to members of AICPA but may be requested by others).

http://infotech.aicpa.org/Resources/Privacy/
AICPA privacy resource page (note that beta "privacy tool" is available only to members of AICPA but may be requested by others).

http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/documents/national_laws/2NATIONAlLAWS_en.asp#TopOfPage
Council of Europe matrix of National Laws on privacy and data protection for European member countries, non-member countries and North America, South America, Asia.

http://www.oecd.org/document/39/0,3343,en_2649_34255_28863271_1_1_1_1,00.html
OECD (Organisation for Economic Co-Operation and Development) Privacy Policy Generator, including guidelines and an interactive policy generator.

http://www.oecd.org/document/1/0,3343,en_2649_34255_28863233_1_1_1_1,00.html
OECD "How to Develop a Privacy Policy" with checklist of questions

http://www2.oecd.org/pwv3/
OECD interactive policy statement generator questionnaire (need to register to begin).

http://www.dmaresponsibility.org/InfoSecurity/
Direct Marketing Association checklist for information security practices.

For an electronic copy the hyperlinks above, please e-mail your request to: jonathan.gordon@alston.com