

Updates to *The Lifeboat Strategy*, 2d ed. (November 2007)

This is the final update for this edition. The 2007-08 edition was published in October 2007

Note: All page numbering refers to the 2006 interim update (May 2006). Page numbering for the second edition (2005) will vary slightly.

p. 10

Replace the third sentence with the following

According to attorney Robert J. Mintz, over 50,000 lawsuits are filed every day in the United States.

p. 12

Replace second paragraph under "Law Enforcement" with

In the United States, the largest law enforcement database is the FBI's National Crime Information Center (NCIC) database. As of 2003, it contained information on 52 million individuals accessed by more than 80,000 law enforcement agencies nationwide. The NCIC serves up information on suspected criminals more than 3.5 million times daily.

p. 13

Replace second paragraph under "Your Identity, There for the Taking," with

Approximately 15 million Americans were victimized by some sort of identity-theft related fraud in the 12 months ending in mid-2006, according to a survey by Gartner, Inc.¹ That's up 50% from the 12-month period ending in mid-2005.

p. 16

Replace first full paragraph with

The 2005 Real ID Act establishes "national uniform standards" for driver's licenses. This will result in national identification cards coming in through the "back door," as you'll learn in Chapter 2.²

p. 18

Add the following paragraph at the end of the discussion of Face Recognition under "Biometrics"

Still, there's no question that face recognition technology is improving. Research published in 2006, sponsored by the National Institute of Standards and Technology, demonstrates that machine recognition of human faces improved tenfold between 2002 and 2006.³

p. 20

Insert the following sentence after the first bullet under "Surveillance and Your PC"

In recent Windows operating systems, the name of the swap file is **page.sys**.

Insert the following in place of the first sentence after the third bullet

All versions of the Windows operating system are insecure, including the newest, Vista.

p. 21

Insert before "Conclusion"

The most recent threat to computer privacy in the United States is a requirement that came into effect in 2007 stipulating that domestic Internet Service Providers make their networks "wiretap friendly."⁴ Essentially, this requires that networks be designed so that an individual's online activity can be monitored by law enforcement authorities without intervention by the network. The requirements apply to universities, public libraries, Internet cafés, and other institutions that operate networks connected to the Internet.

p. 25

Insert following two paragraphs before "Right to Silence"

Preventing welfare fraud is another circumstance where authorities may conduct warrantless searches of a home. In 2006, a federal court ruled that investigators can search welfare applicants' houses without warrants to prevent fraud and ensure they are eligible for assistance.⁵

Replace the last paragraph before "Right to Silence" with

You have a reduced expectation of privacy for activities you carry out away from home, even though you have an interest in keeping information about them out of the public eye. The most visible manifestation of this status is the USA PATRIOT Act's provision for "national security letters," which permit the government to engage in blanket "fishing expeditions" into financial and other business records.

p. 33

Insert prior to "Taxpayer Relief Act (1997)"

Real ID Act (2005)

In 2005, Congress enacted the Real ID Act. Starting in 2013, no state driver's license that fails to conform to federally mandated "minimum standards" can be used for any federal "official pur-

pose," such as boarding an airplane, buying a firearm, obtaining federal benefits, or even entering a federal courthouse. With this requirement, the United States is paving the way for a national ID card and internal passport; two of the ways totalitarian nations track their citizens.

The law's minimum standards require that state driver's licenses be machine-readable. The licenses must also contain your residential address. This data need not be protected in any way; states may publish your home address in plain text on the face of the license. Together, the machine-readable and residential address requirements will make identity theft much easier.

A major selling point of Real ID is that it will be difficult to forge the high-security driver's licenses to be created under its guidelines. However, a hard-to-forge ID card is an extremely valuable document, if its security can be compromised. The record of governments in producing "impossible to forge" ID documents is very poor, as described in Chapter 1.

But perhaps the most threatening aspect of this law is its creation of the equivalent of a national database to include details on nearly 250 million licensed drivers. The database will be created from a series of interlinking systems operated and administered by the states. Each state must provide electronic access to all other states to information contained in its motor vehicle database. An interlinked system is a far greater security risk than a decentralized one with each state issuing ID cards according to its own rules.

Since there's no requirement that the data on your Real ID be protected in any way, private companies are likely to use the information in it at will. Every retailer that requires identification will swipe your Real ID and then sell the data to information aggregators to be data mined at will.

Several states have refused to enforce the Real ID Act due to the high cost of implementing its requirements, estimated at more than US\$23 billion.⁶ While opposition to the law may succeed in minor delays in its implementation, the trend toward a national ID card may be unstoppable.

p. 37

Insert the following immediately before "Data Mining"

Data Aggregators

Almost every piece of personal information that you might want to keep private—your bank statements, your telephone records, and your e-mail messages—is for sale.

As I described in Chapter 1, federal, state and local governments maintain many types of public records. An increasing number of these records are now available over the Internet. The Fair Credit Reporting Act doesn't regulate trade in public records, as data assembled from them are not "credit reports."

Companies such as **ChoicePoint**, **Axiom**, **LexisNexis**, **Westlaw**, and **Seisint** exemplify the evolution of this trade in public records. ChoicePoint, for instance, has compiled more than 20 billion records on virtually every American into a series of searchable databases. These include property records; driver records; motor vehi-

cle records; boating, records of pilot and professional licenses; and court records showing bankruptcies, liens, judgments and divorce. While you're permitted to access some of ChoicePoint's databases under the Fair Credit Reporting Act to insure that the records are accurate, other databases are off-limits. You're not legally entitled to review or make corrections to data that other companies and government agencies—including the FBI—can purchase and use to make decisions about you.

Yet, the reports data aggregators produce are riddled with errors—and in many cases, you have no right to contest them. A 2005 study revealed that **100%** of individuals who obtained a copy of a background check report prepared by ChoicePoint discovered serious errors in it. Most participants found errors in even the most basic biographical information: name, social security number, address and phone number.⁷

Another problem is poor security over the data maintained by data aggregators. In 2005, ChoicePoint sold more than 145,000 of its reports to identity thieves posing as legitimate businesses.⁸

In response to these problems, data aggregators have promised to improve accuracy and security of the reports they provide. ChoicePoint, for instance, is offering free credit reports and a free report-monitoring service to the 145,000 persons whose data was compromised in 2005.

Yet, there is a long way to go. There is little evidence that records maintained by data aggregators are much more accurate than they were in 2005, and state and federal law enforcement agencies still rely on them heavily, with little or no oversight.

Replace the existing section on "Data Mining" with the following text

Data Mining

One of the most innovative ways that information compiled by credit bureaus, data aggregators, and the government is used is through **data mining**. This is a data analysis technique that defines how an individual fits into a group, and predicts behavior based on characteristics of that group.

Direct marketers use data mining to pinpoint consumer tastes. Building upon experience derived from cross-matching government records to ferret out welfare fraud or tax evasion, government agencies today use data mining to analyze thousands of databases containing billions of records of both U.S. citizens and non-citizens alike.

Most people first learned about data mining in 2002, when news of a secret government program called **Total Information Awareness** (TIA) hit the headlines. The idea was simple: compile as much data as possible on as many people as possible from as many data sources as possible, organize it so that it's searchable, then sift through it with super-computers to investigate patterns that might indicate terrorist plots.

Public outrage led to the TIA program being shuttered, yet data mining hardly died. Indeed, according to the General Accountability Office (GAO), as of 2004, there were 122 different federal data mining programs operate that use personal information compiled

by government agencies.⁹ And this is only the tip of the iceberg, because the tally didn't include classified programs like TIA.

The promise of data mining is compelling, and for some purposes, it's very effective. It works best when there's a well-defined profile of whatever you're searching for, a substantial number of "events" (e.g., terrorist attacks, efforts to defraud a government agency, etc.) and minimal consequences for "false positives" (e.g., when the data mining software misidentifies someone as a terrorist, a tax cheat, etc.)

An example of an effective application for data mining is credit card fraud. All credit card companies now data mine their transaction databases, looking for patterns of spending that might indicate a stolen card. Since credit card thieves generally purchase expensive a large number of expensive items in a short period of time, identifying fraudulent use is relatively easy using data mining software.

The same can't be said, unfortunately, when it comes to identifying terrorists through data mining. Terrorists don't fit an easily identifiable profile. Most terrorists are male and under 40. There are nearly two billion people in the world that fit this profile. There are also an exceedingly small number of actual terrorists—probably just a few hundred, perhaps a few thousand at most. And they deliberately obscure their trail to avoid detection. All these factors make data mining to identify terrorism an expensive waste of time.

p. 43

Insert immediately before "Information as Property"

It wasn't supposed to be this way. The original 2001 regulations issued under HIPPA required a patient's consent for most uses "protected health information," including its use for such common activities as treatment, billing and "other healthcare operations."

In 2002, however, the Department of Health and Human Services substituted the words "regulatory permission" for "patient consent," thereby opening the floodgates for the disclosure of previously confidential health information without a patient's consent. As a result of this seemingly small change, according to the Privacy Rights Foundation, some 800,000 companies, government agencies and other organizations can tap into personal medical information almost at will. And they're not required to tell you what they do with it.

Your medical information can be exchanged not only among doctors and other health care providers, but also to "covered entities," including business affiliates of health care organizations such as data clearinghouses, accounting firms, law firms, credit bureaus, and banks.

For instance, a federal rule that went into effect in 2006 allows creditors to obtain or use medical information for determining credit-worthiness. The rule does stipulate that credit-grantors can't use medical data in determining eligibility for a loan or in setting loan terms. However, creditors who have such information can share it with their "affiliates." This converts the data into credit information, not medical data.¹⁰

Chapter 4 contains suggestions on how to protect your medical privacy under the new rules.

p. 45

Insert at bottom of page

This protection is now in question, though, because in 2006, President Bush quietly asserted a new government prerogative to open domestic mail without a warrant, probable cause, or even suspicion that it contains dangerous materials or contraband.¹¹ In addition, since 2002, the Customs Service has been empowered to open international mail without a warrant.

p. 46

Replace second paragraph with

Other privacy advantages enjoyed by first-class mail may be ending as well:

Delete first bullet point

p. 50

Add at bottom of page

- In an "emergency situation" that involves immediate danger of death or serious physical injury to any person, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime, so long as an application for a wiretap warrant is made within 48 hours after a wiretap begins.

p. 51

Add at end of first paragraph

And it continues to this day, in Bush administration's "terrorist surveillance program," which involves unauthorized wiretapping of Americans suspected of communicating with Al Qaeda operatives abroad.¹²

Replace paragraph six with

Only a small number of authorized electronic surveillances occur each year. In 2006, federal and state courts authorized only 1,839 wiretaps,¹³ plus another 2,176 "national security" wiretaps¹⁴ (authorized by a secret court I'll describe momentarily). No applications for wiretap authorizations were denied by either state or federal courts in 2006, although five applications for "national security" wiretaps were later withdrawn. **Note:** These numbers do **not** include wiretaps conducted under the Bush administration's terrorist surveillance program.

p. 52

Insert after paragraph two

A cellular service provider may be able to remotely install software into your cell phone, without your knowledge, that allows the microphone to be remotely activated, converting it into a roving bug. This is possible even if the phone is switched off. This attack is increasingly common in corporate espionage situations but recently was approved for use in criminal investigation.¹⁵ The only way this surveillance method can be defeated is by removing the battery from your cell phone.

pp. 53-54

Replace "Foreign Intelligence Surveillance Act" with:

Foreign Intelligence Surveillance Act (1978)

In its 1967 *Katz* decision, the Supreme Court acknowledged that the president had the inherent authority to order warrantless surveillance in national security investigations. But by the early 1970s, evidence began to accumulate of widespread wiretapping of U.S. citizens by U.S. intelligence services. Hearings in 1975 and 1976 before the U.S. Senate focused on the National Security Agency, America's largest intelligence agency.

Witnesses described initiatives such as **Project Minaret**, in which the NSA monitored dissidents (especially individuals opposed to the Vietnam War) on "watch lists" provided by the FBI, CIA, Secret Service, and the Defense Intelligence Agency. Another major surveillance project was **Shamrock**, in which from 1945 to 1975 U.S. intelligence services inspected all overseas telegrams daily. According to the Committee's final report, Shamrock was the "largest governmental interception program affecting Americans, dwarfing the CIA's mail opening program by comparison."¹⁶

The NSA defended its actions, citing its "inherent presidential authority" to eavesdrop on anyone it viewed as a legitimate foreign intelligence target. In response to these sweeping claims, and to abuses uncovered in its hearings, Congress passed the Foreign Intelligence Surveillance Act (FISA).¹⁷ The statute, until it was temporarily amended in 2007, applied when collecting information about foreign spies or terrorists was "a significant purpose" of surveillance, under one of two scenarios:

- **Without a court order.** Acting through the Attorney General, the President may authorize warrantless electronic surveillance for a period of one year. The surveillance must target only a foreign power or its agents. The purpose of the surveillance must be to gather foreign intelligence information, with no substantial likelihood that the contents of any communication to which a U.S. person is a party will be acquired. FISA also permits the "physical search" of the "premises, information, material, or property used exclusively by" a foreign power. The requirements and procedures for searches are nearly identical to those for electronic surveillance.
- **With a court order.** If a suspected foreign intelligence agent is within the United States, or is communicating with someone within the United States, the NSA (or other investigative agency) must obtain a warrant from a court established under the act: the **Foreign Intelligence Surveillance Court (FISC)**. This court deliberates in secret and its decisions aren't published.¹⁸

The FISC rarely turns down a government wiretap request. Since 1979, it has approved more than 20,000 FISA wiretap requests. But in 2002, the FISC found that in more than 75 cases, the Justice Department had violated federal law in its use of FISA wiretaps. However, its decision was overruled by the U.S. Foreign Intelligence Surveillance Court of Review, which met for the first time ever to review the lower court decision.¹⁹

Numerous examples exist of FBI agents providing inaccurate information to the FISC to obtain FISA surveillance warrants. An internal FBI review in 2006 of the more than 2,000 surveillance warrants the bureau obtains each year confirmed dozens of inaccuracies in court submissions.²⁰

Amendments to FISA enacted in the 2007 **Protect America Act**²¹ temporarily expand the grounds under which the government can conduct intelligence-related surveillance without obtaining a FISA wiretap. This authority ends on Feb. 5, 2008, unless renewed by Congress. The amendments codify into law the "Terrorist Surveillance Program" (TSP) authorized by President George W. Bush in 2001.²²

The TSP appears to take two forms:

- Warrantless wiretaps of conversations originating in, or terminating in, the United States, of individuals allegedly connected to terrorist groups or otherwise of interest to intelligence officials; and
- Mining the data streams of U.S. telecommunications companies to analyze transactional records of telephone and Internet traffic in search of patterns that might point to terrorist suspects.

While billed as essential to fight the "war on terror," the Protect America Act doesn't limit the NSA's domestic spying efforts to terrorist investigations. Instead, all that's required is that "foreign intelligence retrieval" be a "significant purpose" of the surveillance. The law places the authority for such surveillance in the hands of the attorney general—not the FISC. The court's only role is to review surveillance that's already been conducted, and intervene if the procedures set out in the act haven't been followed.

"Foreign intelligence retrieval" encompasses far more than listening in on suspected terrorists. Employees of the White House or the State Department, apparently, were frequent targets of the original TSP, before it was "legalized" in the Protect America Act.²³ In addition, the NSA conducts surveillance on the activities of foreign companies engaged in high-tech research. The results of this surveillance are passed on to politically connected U.S. companies.²⁴

For more information on the NSA's longstanding global surveillance efforts, see Chapter 3.

p. 54

Insert at bottom of page:

Since then, hundreds of companies have gone into business buying and selling private telephone records. One of the most frequently used strategies to obtain someone's phone records is to impersonate that person. Such "pretexting" became illegal in 2006, but persists. Moreover, under U.S. law pretexting is illegal only if carried out by

a private company. Government agencies can continue to impersonate you to obtain your telephone records.

p. 55

Delete the last sentence in paragraph four.

Add to end of paragraph five:

In practice, neither a subpoena nor a warrant is necessary, since it's perfectly legal for investigators to impersonate you in order to obtain your telephone records.

Add at bottom of page:

Another glaring exception applies to e-mail or voice messages stored on an Internet service provider's or telephone company's computers. In most parts of the United States, to obtain this information, the government only has to make a case that the information it is seeking is relevant to an investigation. It doesn't have to establish that there's probable cause of any crime. In the states of Kentucky, Michigan, Ohio, and Tennessee, this information is available only after investigators obtain a search warrant based on probable cause of criminal activity, thanks to a 2007 decision from a federal appeals court.²⁵ However, the ruling applies only in these four states, and has been appealed.

p. 56

Delete paragraph one.

p. 58

Insert after paragraph five

In 2007, CALEA's requirements were extended to the Internet. They now apply to universities, public libraries, Internet cafés, and other institutions that operate networks connected to the Internet. As with other communication networks covered by CALEA, wiretapping the Internet is to occur at the flip of a switch (or perhaps the click of a mouse), without intervention by the network. Comcast Corp., Vonage, and other companies that provide phone service over the Internet are explicitly covered by these provisions.

p. 59

Add following immediately before "USA PATRIOT Act"

Caller ID "spoofing" services now exist and are discussed in Chapter 4. They effectively block transmission of originating telephone numbers, but are under attack by state and federal prosecutors and regulatory agencies.

p. 60

Add following immediately before "The Homeland Security Act (2002)"

Predictably, while the purpose of the USA PATRIOT was purportedly to more effectively protect the United States against terrorism, its primary impact has been in non-terror related investigations. For instance, the courts have made clear that Patriot Act e-mail searches apply to non-terrorists.²⁶ Moreover, a Department of Justice report issued in 2003 cites more than a dozen cases not related to terrorism in which federal authorities have used their expanded powers under the act to investigate individuals, initiate wiretaps and other surveillance, or seize millions in tainted assets.²⁷

In 2006, a report from the Department of Justice's Inspector General's office revealed widespread violations of the use of "national security" and "exigent circumstances" letters. In dozens of cases, agents failed to document relevant evidence, invented emergencies that didn't exist and filed to show that requested records were connected to authorized investigations.²⁸

Also in 2006, several provisions of the act that had been scheduled to expire were renewed.²⁹ These included all of the provisions relating to electronic surveillance.

p. 71

Insert before "Tax Avoidance vs. Tax Evasion"

Circular 230 (2005)

The late 1990s and early 2000s marked a seismic shift in the willingness of wealthy individuals and large corporations to engage in aggressive tax planning. In particular, Big 4 accounting firms started to market tax avoidance plans to clients, often making them sign non-disclosure agreements. The firms would in many cases also provide "opinion letters" stating that the strategy would be likely to withstand a challenge from the IRS, even when the likelihood of prevailing in a dispute was low.

Tax shelters were pervasive in the 1970s and 1980s, but the strategies and marketing used for the latest generation of shelters spurred the Treasury Department to create a strategy that would end the "tax shelter" industry once and for all.

The result was new Treasury Department regulations imposing much higher standards on individuals who provide tax advice, particularly with respect to strategies that might reduce taxes. Published in Circular 230,³⁰ the regulations restrict the ability of tax practitioners to issue "covered opinions" (opinions that taxpayers can use to avoid penalties) and to market tax shelters. Practitioners must also notify the IRS when they create certain types of tax shelters for clients, in so doing identifying the client.

Circular 230 has substantially increased the cost of obtaining tax advice, and substantially reduced the willingness of tax practitioners to engage in aggressive planning. From the Treasury Department's viewpoint, it has been a success.³¹

p. 73

Add after last paragraph

However, BSA filings generally aren't subject to disclosure in civil lawsuits.

p. 75

Add after last paragraph

All U.S. financial institutions, including banks and S&Ls, along with the U.S. Postal Service, must verify a customer's identity and retain a record of the transaction for five years before issuing or selling "monetary instruments" (bank checks and drafts, cashier's checks, money orders and traveler's checks) when purchased with currency in amounts between US\$3,000 and US\$10,000. Many depository institutions restrict sale of these instruments to account-holders and require customers who wish to purchase them in amounts between US\$3,000 and US\$10,000 with currency, to first deposit the currency into their deposit accounts.³²

p. 76

Replace existing text with

BSA Reporting Requirements: Trades and Businesses

The obligation of ordinary U.S. businesses to help enforce the BSA's currency reporting provisions expanded dramatically under terms of the USA PATRIOT Act. If you own a business operating in the United States, and you receive or disburse more than US\$10,000 in currency in a single transaction, or a series of "related" transactions, you're required to file Form 8300. Casinos must complete Form 8362,³³ a modified version of this form. Further, you must notify your customer that you are submitting information on the transaction to the IRS.

In cities that are subject to **Geographical Targeting Orders** (discussed in "Money Laundering Control Act"), businesses may be subject to significantly lower reporting thresholds. For instance, in past GTOs, reporting requirements have been lowered to US\$750 for "money transmitting businesses."

Instructions for Form 8300 state:

Each person engaged in a trade or business who, in the course of that trade or business, receives more than US\$10,000 in cash in one transaction or in two or more related transactions, must file Form 8300. Any transactions conducted between a payer (or its agent) and the recipient in a 24-hour period are related transactions. Transactions are considered related even if they occur over a period of more than 24 hours if the recipient knows, or has reason to know, that each transaction is one of a series of connected transactions.

Note that the reporting obligations apply to transactions only "in the course of that trade or business." If you're a physician, for instance, and someone pays you US\$11,000 in currency for the provision of medical services, you're obligated to complete Form 8300. But if you sell someone a used car for US\$11,000, you're not required to file Form 8300, since the sale occurs outside the course of your trade or business.

Businesses that buy or sell "consumer durables," collectibles, or are engaged in the travel or entertainment industry have expanded reporting obligations. They must report not only transactions in cur-

rency, but in other monetary instruments that constitute what the Treasury Department calls **designated reporting transactions**.

For designated reporting transactions, "cash" not only includes "U.S. and foreign coin and currency received in any transaction," but also, according to Treasury Publication 1544, the following **monetary instruments**:

A cashier's check, money order, bank draft, or traveler's check having a face amount of US\$10,000 or less that is received in a designated reporting transaction (defined below), or that is received in any transaction in which the recipient knows that the instrument is being used in an attempt to avoid the reporting of the transaction.

A **designated reporting transaction** is:

A retail sale (or the receipt of funds by a broker or other intermediary in connection with a retail sale) of a consumer durable, a collectible, or a travel or entertainment activity.

- **Retail sale.** Any sale (whether or not the sale is for resale or for any other purpose) made in the course of a trade or business if that trade or business principally consists of making sales to ultimate consumers.
- **Consumer durable.** An item of tangible personal property of a type that, under ordinary usage, can reasonably be expected to remain useful for at least 1 year, and that has a sales price of more than \$10,000.
- **Collectible.** Any work of art, rug, antique, metal, gem, stamp, coin, etc.
- **Travel or entertainment activity.** An item of travel or entertainment that pertains to a single trip or event if the combined sales price of the item and all other items relating to the same trip or event that are sold in the same transaction (or related transactions) exceeds \$10,000.

Exceptions. *A cashier's check, money order, bank draft or traveler's check is not considered received in a designated reporting transaction if it constitutes the proceeds of a bank loan or if it is received as a payment on certain promissory notes, installment sales contracts, or down payment plans.*

A cashier's check, bank draft, traveler's check, or money order with a face amount of more than \$10,000 is not treated as cash and a business does not have to file Form 8300 when it receives them.

Businesses affected by the BSA must also track installment currency sales. According to federal regulations, "multiple currency deposits" or "currency installment" payments that are "related" are counted as a single transaction. If an initial payment is less than US\$10,000, the business that receives it must track subsequent payments made within one year of the initial payment. If the total aggregate payments exceed US\$10,000 within one year, the transaction must be reported on Form 8300.

p. 81

Replace first two sentences of first full paragraph with

Given the draconian penalties that apply for not filing SARs, it's hardly surprising that the numbers filed are increasing exponentially: from 62,388 in 1996 to 919,230 in 2005, according to FinCEN.³⁴ However, the overwhelming majority of these reports were for innocent activity, as demonstrated by the fact that of the nearly 700,000 SARs filed in 2004, fewer than 900 were actually passed on by the collecting federal agency to a law enforcement agency for follow-up.

p. 92

Insert paragraph beginning, "Are you a racketeer?"

The law relating to the pretrial restraint of substitute assets in criminal forfeiture cases under the relation-back doctrine is not settled. In some judicial districts, prosecutors may restrain substitute assets before conviction or even trial.³⁵ Other federal courts prohibit this tactic.³⁶ The Supreme Court will undoubtedly be called upon to settle this issue.

p. 94

Replace second sentence in paragraph 4 with

The court questioned whether the forfeiture was proportionate to the crime committed, and sent the case back to a lower court for reconsideration.

p. 95

Insert following after second sentence in first full paragraph

However, an alleged RICO violation must be the "proximate cause" of the damages claimed.³⁷

p. 110

Insert at end of third paragraph

The court hearing to authorize the seizure is held in secret, with no notice to the property owner. If the information leading the government to believe the account is subject to civil forfeiture is deemed secret by the government, it may not be possible to find an attorney with the appropriate security clearance to review the evidence.

p. 111

Insert immediately before "Cyberpayments"

An internal FBI audit announced in June 2007 concluded that the bureau illegally used "National Security Letters" more than 1,000 times while collecting data about domestic phone calls, e-mails and financial transactions under the USA PATRIOT Act. The new audit covers just 10% of the bureau's national security investigations since 2002, and so the mistakes in the FBI's domestic surveillance efforts are undoubtedly much higher.

p. 114

Insert in first group of bulleted items:

- **Warrantless wiretaps.** President Bush has acknowledged that under his authority, the NSA wiretapped the conversations of suspected terrorists, without a warrant, as required by law.
- **Monitoring of international money transfers.** The White House has acknowledged that the United States has monitored virtually all international money movements sent through the electronic network in which virtually all such payments are made. No warrant or other legal process is required to obtain this information, merely an administrative subpoena.

p. 116

Insert at the end of paragraph 4

However, you can now be fined up to US\$1,000 **per question** for any census question you don't answer or which you answer "incorrectly."

p. 120

Insert at end of page

But the biggest challenge to the act came in 2006 in the form of amendments to an obscure law dating from 1807, the Insurrection Act. The amendments authorize the President ability to deploy troops within the United States whenever the President determines that the authorities of the state are incapable of maintaining public order. This may occur **without** the consent of state authorities, essentially making the PCA irrelevant.

p. 126

Insert at the end of paragraph 4 under "International Emergency Economic Powers Act"

Civil forfeitures under IEEPA occur administratively, without a court hearing. In 2004, the Supreme Court refused to review a lower court decision upholding this draconian procedure.³⁸

Monitoring of International Money Transfers

Under a secret initiative launched shortly after Sept. 11, 2001, the Bush Administration has gained access to a database of international financial transfers.³⁹ Under authority of the IEEPA, the Treasury Department, under CIA supervision, issued a secret administrative subpoena to compel the Belgian-based Society for Worldwide Interbank Financial Telecommunication, or SWIFT, to open its records. This international banking consortium routes more than US\$6 trillion daily between nearly 8,000 financial institutions worldwide. The use of the IEEPA permitted an end run around U.S. laws that generally require the government to show that specific records are relevant to an investigation of a specific person or group before demanding their release.

U.S. government officials claim that this "Terrorist Finance Tracking Program" (TFTP) investigates only transactions related to ter-

rorist financing, but SWIFT itself says it can't extract the bits of data U.S. analysts seek. So, it has given the Treasury Department access to its entire database of detailed records on billions of bank-to-bank transfers.⁴⁰

As with other data mining programs conducted to fight terrorism, the effectiveness of the TFTP is an open question. Underground networks that exist outside the banking system have long been used in Asian countries to transfer money internationally. Terrorists reportedly use these networks instead of dealing with banks, where their financial dealings are subject to far greater scrutiny.⁴¹

p. 131

Replace paragraphs 2-4 with

Numerous court challenges resulted from these initiatives, and in 2006, the Supreme Court ruled that President Bush overstepped his authority to create military tribunals outside the auspices of the military justice system without congressional approval.⁴² However, Congress shortly thereafter enacted the **Military Commissions Act**, which overruled the court's decision.

Replace "Domestic Political Spying" with:

Despite the Posse Comitatus Act's prohibitions against U.S. military personnel engaging in domestic law enforcement, as summarized earlier in this chapter, the U.S. Department of Defense now conducts domestic surveillance on U.S. citizens.

The impact of this surveillance on catching terrorists is unknown. What is known is that the domestic targets of this program—some aspects of which have now been shuttered—have included anti-war activists staging peaceful demonstrations against military bases and defense contractors. For instance, a California group called the Raging Grannies came under investigation when it helped organize a peaceful demonstration to protest the war in Iraq.

Nor is the Pentagon the only government agency involved in spying on Americans. In 2002, the Department of Justice announced new guidelines that permit the FBI to infiltrate and conduct surveillance on domestic religious and political organizations. The new guidelines loosen one of the most fundamental restrictions on the conduct of the FBI. Controls on the FBI's involvement in domestic political organizations were imposed due to the long history of FBI surveillance and harassment of civil rights and anti-war organizations documented in Chapter 1.

p. 137

Replace the next-to-last paragraph with

In 2006, the U.S. Senate ratified the Convention, but reserved the right to deny cooperation requests when they violate U.S. free speech or other rights.

p. 139

Add after fourth sentence in second paragraph under "The Revenue Rule"

In 2002, the proposal was narrowed so that it would apply only to residents of 15 nations.

Replace last three paragraphs and first two lines on p. 140 with

The revenue rule is also under attack in U.S. courts. There is a longstanding prohibition against the direct enforcement of a foreign tax obligation by a foreign government through the U.S. court system.⁴³ However, the 2005 *Pasquantino*⁴⁴ decision by the Supreme Court appears to open the door to indirect recognition of such claims by U.S. prosecutors applying domestic statutes that indirectly enforce a foreign nation's tax laws.

p. 141

First paragraph:

An updated list of U.S. tax treaties is posted at <http://www.irs.gov/businesses/international/article/0,,id=96739.00.html>.

Replace last paragraph before "Mutual Legal Assistance Treaties" with

As of June 2007, TIEAs were in effect with Antigua & Barbuda, Aruba, the Bahamas, Barbados, Bermuda, the British Virgin Islands, the Cayman Islands, Costa Rica, Dominica, Dominican Republic, Grenada, Guernsey, Guyana, Honduras, the Isle of Man, Jersey, the Marshall Islands, Mexico, Peru, St. Lucia and Trinidad & Tobago. In a handful of these countries, including Mexico and Barbados, ordinary tax treaties are in effect, but in most jurisdictions "encouraged" to sign TIEAs, information flows only one way—to the United States.

Replace third paragraph before "Executive Agreements" with:

As of May 1, 2007, the United States had MLATs in effect with Anguilla, Antigua & Barbuda, Argentina, Australia, Austria, the Bahamas, Barbados, Belgium, Belize, Brazil, British Virgin Islands, Canada, Cayman Islands, Cyprus, Czech Republic, Dominica, Egypt, Estonia, European Union, France, Greece, Grenada, Hong Kong, Hungary, India, Israel, Italy, Jamaica, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Mexico, Montserrat, Morocco, Netherlands, Nigeria, Panama, Philippines, Poland, Romania, Russia, Spain, St. Kitts & Nevis, St. Lucia, St. Vincent & the Grenadines, South Africa, South Korea, Switzerland, Thailand, Trinidad & Tobago, Turkey, Turks & Caicos Islands, Ukraine, United Kingdom, and Uruguay. MLATs with Colombia, Denmark, Finland, Germany, Ireland, India, Malaysia, Portugal, Slovenia, Sweden, Venezuela have been signed, but aren't in force.

Delete last paragraph before "Executive Agreements." The Nestmann Group, Ltd. has withdrawn this publication from its catalog.

p. 145

Delete last sentence in paragraph 2 and replace with:

The IRS ultimately settled 1,165 cases with individual taxpayers for a total collection of US\$3.2 billion—an average of US\$1.7 million per taxpayer.⁴⁵

p. 147

Replace sixth full paragraph with:

A handful of jurisdictions refused to make any concessions to the OECD and remained on its uncooperative tax haven blacklist: Andorra, Liechtenstein, Monaco, Marshall Islands, and Liberia.

In 2006, the OECD published yet another report, entitled *Tax Cooperation: Towards a Level Playing Field: 2006 Assessment by the Global Forum on Taxation*. While this report criticizes previously blacklisted jurisdictions for imposing strict limits on access to bank information in civil tax matters, the OECD's focus has now shifted toward eliminating harmful tax practices in OECD member countries themselves.

p. 148

Delete first sentence under "EU Savings Tax Directive (2001)" and replace with:

The European Union (EU) is a group of 27 European nations, including the largest economies in Europe: France, Germany, Italy, and the United Kingdom.

p. 148-149

Replace last paragraph on p. 148, continuing to p. 149, with:

In 2003, a compromise proposal blending information exchange and withholding received the unanimous support required to come into effect. While most member states began sharing information in 2005, Austria, Belgium and Luxembourg now impose a withholding tax on non-residents' savings and hand back 75% of the proceeds to their countries of origin. The tax started at 15% in 2005, rose to 20% in 2007 and will increase to 35% in 2010. Crucially for the plan, both Switzerland and Liechtenstein have agreed to participate.

p. 150

Insert before first full paragraph:

In 2006, the United Nations renewed its initiative to impose global taxes in a new report that proposes taxation of air transport and airline tickets, currency transactions, carbon emissions (gasoline) and arms sales. Media reports state the initiative enjoys wide support among international trade unions, environmental groups, and NGOs.⁴⁶

p. 152

The Web site for the Financial Action Task Force is now at <http://www.fatf-gafi.org>.

p. 153

Add the following immediately before "Global Anti-Laundering Network"

More recently, the FATF has indirectly criticized the United States for failing to require mandatory registration of all trusts and mandatory disclosure of trust beneficiaries. The FATF has also called for the global elimination of the possibility for anonymous ownership of business entities, as is possible with some U.S. corporate forms.⁴⁷

p. 154

Paragraph 2 under "The FATF Blacklist (2000)"

No countries remain on the FATF blacklist.

p. 158

Replace paragraph under first set of bullets with:

In 2005, the European Parliament approved a Third Directive intended to amend and consolidate the previous two laundering directives. All EU members must put the following measures into effect in their domestic law by the end of 2007:

Delete first bullet point.

p. 159

Replace paragraph under the first set of bullets, the second set of bullets, and the next paragraph with:

The size of the offshore industry is staggering. According to a 2005 study by the Tax Justice Network, approximately US\$11.5 trillion of assets are held offshore by high net-worth individuals.⁴⁸ These private funds are held primarily in offshore banks, trusts, and mutual funds. To this figure must be added trillions more in corporate offshore assets: captive insurance companies, shipping companies, and the foreign subsidiaries of multinational corporations.

p. 160

Insert the following sentence at end of paragraph immediately before "The Crown":

A Mareva injunction issued in one country may be enforced in any other country with an English common law background that has incorporated this injunction into its law.⁴⁹

p. 171

Insert before "Keep a Small Circle of Friends"

Especially keep your mouth shut with respect to anything you say to a representative of the federal government. It is a felony under the federal perjury statute, punishable by fines and imprisonment, to lie to a duly authorized representative of the U.S. government.⁵⁰ You can still be punished even if the lie is oral and not under oath, if the agent has not warned of the consequences of lying, if you are not trying to cheat the government or even if the agent is not misled by your deception. Billionaire Martha Stewart is one of thousands

of defendants who have been convicted and imprisoned for violating this law.

p. 173

Insert after last bullet point:

- **Use asset protection trusts (APTs).** A well-drafted APT that names your spouse as a beneficiary is an excellent way to keep your property separate from your spouse's property. This is especially important in community property states. (APTs are discussed later in this chapter). In addition, an APT is a much more subtle way of protecting your property than a pre-nuptial agreement in that it doesn't shout to your spouse, "I don't trust you." However, your spouse probably won't realize that in a typical APT, he or she can be removed as a beneficiary.

p. 175

Add the following bullets before the paragraph beginning, "If you believe..."

- **Protect yourself from "pretexting."** One of the ways that identity thieves (along with lawyers, government investigators, and others) can gather information about you is to impersonate you when dealing with someone who has access to your data. While it became illegal in 2007 for private investigators to use pretexting to obtain telephone records, impersonating someone to obtain other types of records remains perfectly legal. To protect yourself from pretexting, use a disposable phone (described later in this chapter) to prevent your calling records from falling into the wrong hands. Also, assign a hard-to-guess password (not your SSN) that anyone who contacts utility companies, banks, credit card companies, etc. must disclose in order to retrieve your personal data.
- **Place a credit freeze on your credit bureau account.** This action "locks" your credit file, prohibiting new extensions of credit being issued in your name. When you sign up for a credit freeze, you're assigned a PIN with which you can lift the freeze when necessary. About 30 states now authorize credit freezes. All three credit bureaus now offer credit freezes.

Add the following bullets after the paragraph beginning, "If you believe..."

- **File a police report.** Some creditors may want to see a copy of a police report as "proof" that you're a victim of identity theft.

p. 179

Add the following bullet after the first two bullets:

- If police receive consent to search from a resident of the home. However, police cannot search when one resident invites them in but another tells them to go away.⁵¹

p. 180

Delete first and fourth bullets. Replace third bullet with:

- **Mail Preference Service.** Contact this service to reduce the amount of unsolicited commercial mail ("junk mail") you receive from members of the Direct Marketing Association. There is a US\$1 fee for this service. Register online at <https://www.dmaconsumers.org/cgi/offmailing> or write to Direct Marketing Association, P.O. Box 282, Carmel, N.Y. 10512.

p. 182

Add the following at end of list of bullets:

- **Check the routing of international correspondence not originating or being delivered to a U.S. address to insure it doesn't pass through the United States.** Many packages mailed to or from Canada, Mexico, or South America pass through the United States on their way to Asia or Europe. If the package passes through the United States, it can be opened for warrantless inspection by U.S. Customs of Homeland Security authorities.⁵² Ask your carrier if a package you're mailing to and from a non-U.S. address will pass through the United States. If it does, try to find a carrier that doesn't route through the United States.

p. 185

Insert at end of first paragraph under "Protect Telephone Privacy:"

The proposed SAFETY Act would require U.S. telecoms to retain records of telephone calls made or received for at least one year.

p. 186

Insert immediately before sixth full paragraph:

If you opt not to take these precautions, contact your telephone carrier (both land lines and cell phones) and request that call details be removed from your bills. To prevent the carrier from selling your calling records, tell the company you want to "restrict" or "opt out" from all **CPNI sharing**. Place a password on your account to prevent access by someone impersonating you. Finally, instruct the telephone companies to deactivate online access to your account. Information brokers often obtain cell phone records by setting up online account access that customers have not themselves activated.

Insert immediately before "Protect Cordless and Cellular Phone Conversations"

Legislation to ban spoofing services is now pending in Congress.

p. 232

Replace the last three paragraphs with:

Many other types of retirement plans are not ERISA-qualified, including IRAs and simplified employee pension (SEP) plans. However, the 2005 Bankruptcy Reform Act exempts from creditor attachment IRAs and other non-ERISA-qualified retirement plans or contracts similar to those plans covered by ERIS. For IRAs, these plans are protected up US\$1 million maximum value.

You must declare bankruptcy to gain this protection. That means creditors can seize property that isn't exempt under bankruptcy laws. For instance, a personal residence that would otherwise be protected under a state's homestead laws may be seized in a bankruptcy proceeding if you've owned it for fewer than 1,215 days, unless your equity in it doesn't exceed specified limits (for 2007, US\$136,875). Further, spousal and child support claims aren't exempted; nor are claims from the IRS.⁵³ IRAs may also be seized in criminal forfeiture cases.⁵⁴

An innocent spouse living in a community property state⁵⁵ may also lose his or her community property interest in an ERISA-qualified plan to non-exempt creditors.⁵⁶

p. 237

Replace third sentence in the first full paragraph with:

It's also much more difficult for a successful litigant to collect against offshore assets. In some countries, it is impossible for a U.S. litigant to collect a judgment without bringing a new suit, although other countries will enforce U.S. judgments in certain circumstances.

p. 242

Insert the following paragraphs immediately before "Custodial Accounts"

In recent years, the IRS has required offshore banks which hold U.S. dollar in the United States to execute "qualified intermediary" (QI) agreements intended to identify U.S. persons trading U.S. securities without paying tax on any income or gain from such trade. The QI agreement may require the offshore bank to prohibit transactions in foreign securities if the trading instructions originate in the United States. The agreement may also prohibit the offshore bank from making its buy/sell recommendations available to U.S. persons.

Such restrictive QI agreements have the effect of making offshore banking much less useful to U.S. residents—and perhaps that is part of the reason they exist. Fortunately, by doing business with an offshore bank that has minimal contacts with the United States, you can often avoid these restrictions—although such banks are more difficult to find than they once were.

p. 243

Delete last paragraph before "Precious Metals Accounts" and insert:

U.S. Tax Traps in Offshore Funds

One of the most confusing aspects of offshore investing is the U.S. tax treatment of offshore mutual funds and offshore unit investment trusts.

When you purchase a U.S. mutual fund, your income or gain is passed through to you in proportion to your holdings and reported to the IRS on Form 1099. Since offshore funds and unit trusts don't file Form 1099, the IRS requires investors in these contracts to determine their share of the income and pay tax on it. This isn't always easy to do. And if it's not possible to make the necessary calculations, using IRS-approved methods, the IRS imposes punitive taxes and interest payments on whatever taxes are deferred.

The U.S. Tax Code refers to offshore funds organized as corporations as **passive foreign investment companies (PFICs)**.⁵⁷ You'd think the IRS would make it easy to avoid deferring income or gain in a PFIC. But that's not possible unless the PFIC qualifies under one of two sets of rules.

1. U.S. investors in PFICs that choose to be what the IRS calls **qualified electing funds (QEFs)** may pay taxes at **ordinary income tax rates** on their income or gain each year. (Dividend income and long-term capital gains from offshore funds are **not** eligible for the 15% tax rate for applies to most dividends or capital gains.) However, the QEF rules are available only to offshore funds willing to submit to the jurisdiction of the U.S. Securities and Exchange Commission and to comply with U.S. accounting standards. The funds must also agree to allow U.S. investors to inspect and copy any records necessary to calculate income and capital gains in accordance with these rules. The overwhelming majority of offshore funds aren't willing to do so for the sake of U.S. shareholders. **As a result, very few offshore funds qualify as QEFs.**

2. A second set of rules, the **mark-to-market** rules, apply to closed-end funds traded on a qualifying securities exchange. Under these rules, U.S. investors again pay tax at ordinary income tax rates on income or gain from the fund during the year. A long list of requirements must be met for this exception to apply, but many offshore funds traded on major securities exchanges appear to qualify. However, no official list of approved countries or exchanges exists.

If an offshore fund doesn't qualify under either the QEF or mark-to-market rules, it is deemed a "Section 1291 Fund," after the section of the U.S. Tax Code describing its unique tax treatment. At first glance, treatment as Section 1291 Fund seems ideal because you're not generally required to pay any income tax until you sell, other than income tax at your marginal rate on any income or capital gains actually distributed to shareholders).

The IRS regulations interpreting Section 1291 are hideously complex, but the results are basically as follows:

- When tax is paid, all income and gains are taxed at the highest ordinary income rate bracket that applies (presently 35%), not your actual tax bracket.
- All losses are non-deductible.
- You must calculate gains as if they were made evenly, for each year that you held the fund.
- An interest charge applies for each year tax was deferred on these gains. As of early 2007, this rate was around 8%.⁵⁸

For offshore funds held for many years, the tax and interest due can easily exceed the total gain. However, the law provides that the tax and interest charge shall not exceed the amount of the distribution.

Most offshore banks aren't familiar with these rules. U.S. investors in offshore funds who don't report and pay tax on income or gain each year will generally come under the PFIC rules, and can wind up owing huge amounts of interest to the IRS for the "privilege" of deferring taxes due.

In addition to these draconian provisions, U.S. investors in PFICs must also complete IRS **Form 8621** each year in which they generate income or gain from an offshore fund, and report it as ordinary income on their tax return. This form is relatively easy to complete for offshore funds that qualify for QEF or mark-to-market treatment. But for Section 1291 funds, you'll likely require an accountant familiar with the PFIC rules to complete the form.

Three Ways U.S. Investors Can Safely Purchase Offshore Funds

There are three ways U.S. investors can avoid the draconian PFIC regulations:

1. Purchase offshore funds through IRAs and other types of pension or profit-sharing plan
2. Purchase offshore funds through a variable annuity
3. Purchase offshore funds through a life insurance policy.

Here are the details:

Purchasing offshore funds through a retirement plan. Income or gain within a retirement plan isn't taxed until it's paid out to the beneficiary or beneficiaries, at which time it's taxed as ordinary income. There's no provision within the U.S. Tax Code for income or gain from offshore funds to be taxed any differently, offering a convenient way to avoid the PFIC rules.

As long as the retirement plan is administered according to U.S. law, the investment selection and location where they're kept is mostly up to you—or the plan administrator if you don't have a self-directed plan. There is no prohibition against a retirement plan owning offshore funds. This is true of both "**qualified**" plans under the 1974 ERISA law and "**non-qualified**" plans (e.g., IRAs and SEPs).

For this strategy to work, you must have: 1) a self-directed plan; and 2) a U.S. custodian willing to purchase offshore funds or other "non-traditional" investments.

Determining whether a non-self-directed plan can be made self-directed requires an inquiry to the plan administrator. If it can be made self-directed, you'll want to make sure that no tax is triggered upon a "rollover" to a self-directed plan. (In most cases, the answer is no, but ask an accountant to make sure.)

Next, you need to find a U.S. custodian willing to purchase offshore funds or other "non-traditional" investments. Most approved custodians prohibit foreign investments in the retirement plans they administer. It's a business decision they've made—but it has nothing to do with the law.

Unfortunately, there are few U.S. custodians willing to hold foreign investments and offshore funds in particular in U.S. retirement plans. They don't advertise this fact to avoid the possibility of having Congress or the IRS rewrite the rules to prohibit this strategy.

Purchasing offshore funds through a variable annuity. Under U.S. tax law, a variable annuity serves as a tax-deferred "wrapper" for an underlying investment account. Income or gain in the account isn't taxed until it's actually distributed to the beneficiary. Again, there's nothing in the U.S. Tax Code subjecting offshore funds held within a variable annuity to a different standard (assuming the variable annuity is designed to be U.S. tax compliant). As with any other investment wrapped in the annuity, income or gains from offshore funds are tax deferred, without the PFIC interest charges, until the income is repatriated.

The problem once again is that U.S. insurance companies aren't willing to issue variable annuities permitting the purchase of offshore funds. However, numerous offshore insurance companies offer IRS tax-compliant variable annuities that routinely hold offshore funds in their investment accounts. Minimum policy sizes for this strategy to be practical start around US\$50,000. Unfortunately, due to state and federal insurance licensing and securities laws, these companies are not permitted to market themselves to U.S. investors. It may also be necessary to travel to the country where the annuity contract is issued to put it into force.

Purchasing offshore funds through a life insurance policy. A life insurance policy provides the benefits of a variable annuity and more: the death benefit received by beneficiaries is not subject to income tax. The use of an irrevocable life insurance trust can make the death benefit free of estate and generation-skipping taxes as well. **In other words, taxes on the income or gain within the investment account are eliminated.**

A few U.S. life insurance companies will issue "private placement" policies to high net worth clients that permit the purchase of offshore funds. However, very high minimums (US\$5 million or more) are the norm. Offshore, the minimums for this strategy are much lower (typically US\$500,000). But again, offshore insurance companies can't advertise this strategy, and you may need to sign the insurance contract in the country where it's put into force.

WARNING: In order for a foreign variable annuity or life insurance contract to be "qualified" for U.S. tax purposes, stringent IRS requirements must be followed. For instance, the U.S. policyholder is not permitted to make decisions regarding the holdings within the investment account, although it is possible to request that a particular advisor or investment strategy be followed. Consult with a qualified international tax advisor to confirm that any policy offered by an offshore insurance company is U.S. tax compliant.

If you're interested in implementing one or more of these strategies, please contact The Nestmann Group for more information. We can assist U.S. persons in setting up tax-compliant offshore structures to purchase offshore funds and other international investments.

p. 252

Replace the paragraph beginning with "Money orders..." with:

Money orders were once a good way to fund offshore bank accounts in relative privacy. However, the Bank Secrecy Act now requires U.S. issuers of money orders to maintain the names, addresses, and Social Security numbers of individuals who purchase more than US\$3,000 of money orders at one time. In addition, fewer foreign banks are willing to accept U.S. money orders except (possibly) from known customers. If you want to fund your account with money orders, make certain the bank will accept them.

Replace the second paragraph under "Personal or business checks" with:

In years past, it was common to fund an offshore bank account with an endorsed third-party check. This is a check made payable to you that you endorse and then transfer to someone else by endorsing it and then writing "pay to the order of" that person—in this example, your offshore bank. However, most offshore banks no longer accept endorsed third-party checks, and the practice is even prohibited in some offshore jurisdictions. While a check endorsed to a foreign account doesn't appear to be a "monetary instrument" subject to BSA reporting requirements, U.S. banks have been alerted that it may constitute a "suspicious transaction." For this reason, avoid using endorsed third-party checks to fund an offshore account.

p. 255

Insert immediately before "What is reportable?"

WARNING: If you have unreported foreign bank accounts, you should immediately seek legal counsel from a criminal tax attorney. It is possible that working a criminal tax attorney, you can work out an arrangement with the IRS to file the appropriate tax returns, pay the taxes, penalties, and interest and avoid criminal prosecution.

p. 256

Replace fourth bulleted item

- **Warehouse receipts and similar instruments.** Certificates that represent ownership of a specified quantity of precious metals or other commodity, stored outside the United States, may not be reportable. A certificate should provide for "allocated" or "non-fungible" storage to qualify in this regard. This means you own specific barrels, bars, coins that are stored in your name and not available to meet other claims of the warehouse company. Commodities held in non-allocated, pooled, or fungible form may be reportable.

p. 258

Insert after first set of bullets:

Each QI agreement is different. Some foreign banks, particularly institutions with U.S. branches, have QI agreements that require Form W-9 to be filed for any U.S. client who purchases any securities, U.S. or non-U.S. If a bank doesn't require Form W-9, it will request that you complete a form stating that you don't intend to hold U.S. securities in the account.

The same policies may extend to corporate accounts in a U.S. person has direct or indirect ownership. In the case of offshore trusts, the IRS takes the position that Form W-9 is required when the trust has a U.S. grantor and the trust opens a foreign account that purchases any kind of securities.

Foreign banks aren't required to disclose the identities of non-U.S. investors in custodial accounts to the IRS. However, non-U.S. depositors must complete **Form W8BEN** to certify non-U.S. status. Otherwise, **all income and gross sales proceeds are subject to a 30% withholding tax.** Similarly, a non-U.S. company or trust operating a non-U.S. account with no U.S. beneficial owners must file IRS Form W8BEN when it purchases U.S. securities. This form certifies its non-U.S. status.

One of the most effective strategies to avoid the QI regime is to invest in offshore variable annuities and offshore variable life insurance contracts generate legally tax-deferred income. I'll discuss this option in greater detail later in this chapter.

Delete the paragraph before the last set of bullets and the bullets themselves.

p. 260

Delete the last paragraph on this page.

p. 267

Rephrase last sentence before "Structuring an APT:"

In general, OAPTs should not purchase offshore funds unless the interests are held in a tax-deferred vehicle such as a life insurance policy.

p. 275

Insert the following before the last paragraph:

One small consolation is that the CFC and PFIC regimes generally don't apply simultaneously; if a foreign corporation is subject to CFC provisions, it's not subject to the PFIC rules on the same income, and vice-versa.⁵⁹

p. 281

Delete first paragraph. This title is no longer sold by The Nestmann Group.

p. 290

Second paragraph under "Live Offshore:"

Replace \$80,000 with \$85,700 and \$160,000 with \$171,400.

p. 292

Replace the text on this page beginning with paragraph five with:

Congress first imposed **anti-expatriation rules** penalizing U.S. citizens who gave up their citizenship for tax avoidance reasons in the 1960s, tightening them in 1996 and 2004. Currently, the U.S. Tax Code imposes income and estate taxes for 10 years after an individual gives up their U.S. citizenship. Also covered are permanent resident aliens ("green card" holders) or anyone else who has resided in the United States for any eight of the preceding 15 years.⁶⁰

The rules apply only to the net combined amount of U.S. source income and income "effectively connected" with a U.S. trade or business. They establish a presumption that persons giving up their U.S. citizenship after June 4, 2004 do so for tax avoidance purposes if they had assets of more than \$2 million or paid more than \$620,000 in federal income taxes over the five years before leaving. Only certain dual citizens and minors with few ties to the U.S. can get exemptions from these rules. However, with proper planning, it's relatively easy to avoid U.S. taxes for the 10 years after expatriation.⁶¹

Because the anti-expatriation rules are not difficult to circumvent, there have been periodic calls to make them stricter. The proposal most often repeated is for an **exit tax**; any expatriate

p. 293

Replace first partial paragraph with:

with a net worth above a certain threshold would be subject to a tax on unrealized gains, to be paid at the time of expatriation. Exit tax bills were first introduced in 1995 and the idea resurfaces in almost every congressional session. The ferocity with which politicians have seized upon the issue of a few wealthy Americans giving up their citizenship each year to save on taxes probably equates to an eventual tightening in the law.

The most recent exit tax proposal, which was passed by the Senate in 2007, but not by the House of Representatives, would replace the existing anti-expatriation rules with an exit tax due within 90 days of relinquishing U.S. citizenship or long-term residence on all unrealized gains worldwide at their fair market value. The first US\$600,000 of gains would be excluded (US\$1.2 million in the case of married individuals filing a joint return, both of whom relinquish citizenship or terminate long-term residence). Most extraordinarily, the immigration rules that deny tax-motivated expatriates entry into the United States would be modified to remove the requirement that the relinquishment be tax-motivated. Instead, former citizens would be denied entry if not in full compliance with U.S. tax obligations. The punitive nature of this proposal is underscored by the fact that the tax will generate only an estimated US\$251 million over the five-year period after enactment.⁶²

The Nestmann Group offers a report analyzing the proposed U.S. exit tax and its potential impact on wealthy U.S. citizens and long-residents. For more information, see http://www.nestmann.com/catalog/product_info.php?cPath=21&products_id=43.

pp. 294-295

Replace the two bulleted items on the bottom of p. 294 and the one

bulleted item on the top of p. 295 with:

- **Commonwealth of Dominica.** Under this country's economic citizenship program, you may acquire citizenship and passport in return for a cash contribution of US\$75,000. A US\$100,000 contribution entitles you, your spouse, and two minor children to citizenship. Legal and processing fees add approximately US\$30,000 to the cost. Dominican passport holders can travel without a visa, or obtain a visa upon entry, to nearly 90 countries and territories. Travel to the United States, however, requires a visa.
- **Federation of St. Kitts & Nevis.** Applicants for economic citizenship must invest US\$350,000 in an approved real estate project. In addition, applicants must pay a registration fee of US\$35,000 for a main applicant and US\$15,000 for each spouse and dependent child under 18. Alternatively, you may make a contribution to the Sugar Industry Diversification Foundation. The cost for a single applicant under this option is US\$200,000, or US\$250,000 for an applicant with up to three dependants, and there is no registration fee. Legal and processing fees add approximately US\$30,000 to the cost. St. Kitts & Nevis passport holders can travel without a visa, or obtain a visa upon entry, to more than 90 countries, but not to the United States.
- **Austria.** It is also possible, although in most cases very expensive, to obtain "instant" Austrian citizenship through an economic contribution. Only a handful of persons gain citizenship in this manner every year. The Austrian program is fundamentally different from that of Dominica and St. & Nevis, however, in that you must make your investment first and then apply for citizenship. You don't get your money back if citizenship isn't granted. Generally, you must invest at least €3 million to have a reasonable chance at qualifying, and pay additional legal fees of at least €400,000 for the main applicant, and a minimum of €50,000 per dependent (spouse and children under 18). However, this program is politically unpopular and it is increasingly difficult to obtain citizenship under this option. It appears likely the program will eventually be terminated.

The Nestmann Group, Ltd. can provide introductions to qualified practitioners in countries that offer economic citizenship. Please contact us for more information.

p. 295

In the next-to-last paragraph, replace the URL listed with <http://www.ind.homeoffice.gov.uk/lawandpolicy/immigrationrules>.

pp. 304-307

The list of titles sold by The Nestmann Group, Ltd. has been updated. Please go to the bookstore at <http://www.nestmann.com/catalog/default.php> for the latest list of titles, or download our catalog at http://www.nestmann.com/pics/archive/nestmann.com_catalog.pdf.

Notes

- ¹ "Identity Theft Up 50%," *Technology News*, March 7, 2007.
- ² "New Law Furthers De Facto National ID Card." *Privacy Journal*, January 2005.
- ³ Mark Williams, "Better Face Recognition Software." *Technology Review*, May 30, 2007
- ⁴ Kevin Poulsen, "Reminder: Monday is Wiretap the Internet Day." *Wired*, May 11, 2007
- ⁵ *Sanchez vs. San Diego County*, Case No. 04-55122 (9th Cir., Sept. 19, 2006).
- ⁶ Spencer S. Hsu, "Cost and Privacy Concerns Cited In New Rules for Driver's Licenses" (*The Washington Post*, March 2, 2007).
- ⁷ "PrivacyActivism Study Finds New Problems for ChoicePoint, Acxiom" (Press release from PrivacyActivism, May 19, 2005).
- ⁸ Kim Zetter, "ID Theft Victims Could Lose Twice" (*Wired News*, February 22, 2005).
- ⁹ "Data Mining: Federal Efforts Cover a Wide Range of Uses." GAO-04-548 (General Accounting Office, May 2004).
- ¹⁰ Regulation Allows Potential Creditors Access to Medical Records." *The Denver Business Journal*, April 7, 2006.
- ¹¹ James Gordon Meek, Bush Says Feds Can Open Mail Without Warrant,." *New York Daily News*, Jan. 4, 2007.
- ¹² James Risen, "Administration Pulls Back on Surveillance Agreement." *The New York Times*, May 2, 2007.
- ¹³ 2006 Wiretap Report, Administrative Office of the United States Courts, April 30, 2007.
- ¹⁴ *FISA Annual Public Report* (2006)
- ¹⁵ *United States vs. Tomero*, Case No. S2 06 Crim. 0008 (LAK) (U.S. District Court, S.D. New York, Nov. 27, 2006).
- ¹⁶ "Intelligence Activities and the Rights of Americans," *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities* (U.S. Senate, April 26, 1976).
- ¹⁷ Pub. L. 95-511, 92 Stat. 1783 (1978)
- ¹⁸ "Foreign Intelligence Surveillance Act: Frequently Asked Questions (and Answers)" (Electronic Frontier Foundation, undated).
- ¹⁹ "Ruling Eases Restrictions On Terror-Suspect Pursuit" (*The Wall Street Journal*, Nov. 19, 2002).
- ²⁰ John Solomon, "FBI Provided Inaccurate Data for Surveillance Warrants" (*The Washington Post*, March 27, 2007).
- ²¹ Pub. L. 110-55, 121 Stat. 552 (2007).
- ²² James Risen & Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts" (*The New York Times*, Dec. 16, 2005.)
- ²³ Jason Leopold, "NSA Spying Evolved Pre-9/11" (OpEd News, Jan. 17, 2006).
- ²⁴ "U.S. Echelon Spy Network a Fact, European Parliament Told" (Agence France-Presse, Sept. 5, 2001).
- ²⁵ *Warshak v. United States*, Case No. 06-4092, U.S. Sixth Circuit Court of Appeals (June 18, 2007).
- ²⁶ Josh Gerstein, "Patriot Act E-Mail Searches Apply to Non-Terrorists, Judges Say." *The New York Sun*, Feb. 28, 2006
- ²⁷ Eric Lichtblau, "Patriot Laws Used Against Non-Terrorists." *The New York Times*, Sept. 28, 2003.
- ²⁸ *A Review of the Federal Bureau of Investigation's Use of National Security Letters*. U. S. Department of Justice, Office of the Inspector General, March 2007.
- ²⁹ USA PATRIOT Improvement and Reauthorization Act of 2005 (P.L. 109-177, Mar. 9, 2006).
- ³⁰ "Regulations Governing the Practice of Attorneys, Certified Public Accountants, Enrolled Agents, Enrolled Actuaries, and Appraisers before the Internal Revenue Service." 31 C.F.R. (A)(10), June 20, 2005.
- ³¹ Stephen L. Feldman, "Alert Regarding Treasury Department Circular 230 Regulations Providing Standards for Written Federal Tax Advice and Sanctions for Noncompliance." *Mondaq.com*, June 16, 2005.
- ³² 31 C.F.R. §103.29.
- ³³ Forms 8300 and 8362 are available at http://www.fincen.gov/reg_bsaforms.html.
- ³⁴ *The SAR Activity Review—by the Numbers*, Issue 7 (Financial Crimes Enforcement Network, November 2006)
- ³⁵ *In re Billman*, 915 F.2d 916 (4th Cir. 1990).
- ³⁶ *United States vs. Gotti*, 155 F.3d 144, 145 (2d Cir. 1998).
- ³⁷ *Anza vs. Ideal Steel Supply Corp.*, Case No. 04-433 (U.S. Supreme Court, June 5, 2006)
- ³⁸ "Faith, Hope, Charity and Terror Charges," *The National Law Journal*, March 12, 2004.
- ³⁹ "Bank Data Sifted in Secret by U.S. to Block Terror" (*The New York Times*, June 23, 2006).
- ⁴⁰ Greg Miller & Josh Meyer, "World's Banks Let U.S. Plumb Books" (*The Chicago Tribune*, June 24, 2006).
- ⁴¹ "Hawala: An Alternative Banking System and Its Connections To Blood Diamonds, Terrorism, and Child Soldiers" (TED Case Studies No. 119, 2003).
- ⁴² *Hamdan vs. Rumsfeld*, Case No. 05-184 (U.S. Supreme Court, June 29, 2006).
- ⁴³ *Restatement (Third) Of Foreign Relations Law* § 483 (1987).
- ⁴⁴ *Pasquantino vs. United States*, 544 U.S. 349 (2005)
- ⁴⁵ Cynthia Blum, "Sharing Bank Deposit Information with Other Countries: Should Tax Compliance or Privacy Claims Prevail?" *Florida Tax Review*, vol. 6, p. 579 (2005)
- ⁴⁶ "What If There Were an International IRS?" *National Review*, March 10, 2006.
- ⁴⁷ *The Misuse Of Corporate Vehicles, Including Trust And Company Service Providers* (FATF, 2006).
- ⁴⁸ "The Price of Offshore." Tax Justice Network (2005).
- ⁴⁹ Jeremy Walton, "The Enforcement of Asset-Freezing Orders Abroad." *Mondaq.com*, August 11, 2006.
- ⁵⁰ 18 U.S.C. 1001
- ⁵¹ *Georgia vs. Randolph* (Case No. 04-1067, U.S. Supreme Court, March 22, 2006).
- ⁵² Diane Francis, "Whose Mail is it Anyway?" *Financial Post*, March 14, 2007.
- ⁵³ *United States vs. Sawaf*, 74 F.3d 119 (6th Cir. 1996).
- ⁵⁴ *United States vs. Vondette*, Case No. 02-1528, 02-1529 (2d Cir. Dec. 16, 2003).
- ⁵⁵ Arizona, California, Idaho, Louisiana, Nevada, New Mexico, Texas, Washington, and Wisconsin are community property states. Several other states stipulate that all property acquired and income earned during marriage is considered marital property and subject to "equitable distribution." Equitable doesn't always mean equal, although 50-50 is the norm.
- ⁵⁶ *In re McIntyre*, 222 F.3d 655 (9th Cir. 2000).
- ⁵⁷ This is a slight simplification. A PFIC is any foreign corporation that earns at least 75% of its income through "passive" investments (interest, dividends, passive rents, royalties, capital gains, commodity gains, and currency gains) OR that holds 50% or more of the average value of its assets for the generation of passive income. Since most offshore funds generate income exactly this way, the overwhelming majority of them are PFICs.
- ⁵⁸ The interest charge on deferred excess distributions from PFICs is based on the "Applicable Federal Short Term Rate" published by the IRS for each calendar quarter, plus 3%.
- ⁵⁹ I.R.C. § 951(d)
- ⁶⁰ 26 U.S.C. 877.
- ⁶¹ For a review of planning strategies under the current U.S. expatriation rules, see Emmanuelle Lee, "Will the Renunciation of U.S. Citizenship Still be Worth Some Tax Savings? An Analysis of the Recent Reform on the Taxation of Expatriates." *Santa Clara Law Review* (vol. 37, 1997), pp. 1063-1105.
- ⁶² Charles Bruce, Lewis Saret, Stéphane Lagonico & Steve Trow, "The Exit Tax—A Perfectly Bad Idea." *Tax Notes International* (2006), p. 867 (p. 868).