

Updates to *The Lifeboat Strategy*, 3d ed. (February 2008)

The 3d edition was published in October 2007

*Note: All page numbering refers to the THIRD edition of *The Lifeboat Strategy*. The final update for the SECOND edition is published at http://nestmann.com/pdf/lifeboat_updates_1107.pdf.*

p. 17

In January 2008, the FBI proposed a global network, through which U.S. law enforcement and intelligence agencies would have direct access to biometric information held in foreign databases. The proposal would, for the first time, expand the five-nation UK-USA intelligence sharing agreement (Chapter 2) between the United States, the United Kingdom, Canada, Australia, and New Zealand, into regular law enforcement.¹

p. 46

Additional details of warrantless domestic surveillance by U.S. intelligence agencies have emerged. Warrantless wiretapping in numerous non-terrorist situations has been documented since the mid-1990s, and possibly earlier. Essentially the National Security Agency (NSA) has installed equipment in the network hubs of most major telecom companies which routes all telephone and Internet traffic through NSA computers. This is done without a search warrant or any judicial oversight whatsoever.²

p. 49

Law enforcement agencies now routinely seek real-time tracking data from cell phone companies so they can pinpoint the whereabouts of criminal suspects. In many cases, no warrant is necessary to obtain this data.³

p. 54

The official name of the Cybercrime Treaty is the Council of Europe's Convention on Cybercrime. In December 2007, a federal judge in Vermont ruled that prosecutors cannot force a criminal defendant to divulge his encryption passphrase. This decision runs contrary to the intent of the cybercrime treaty. It also conflicts with laws in the United Kingdom and other countries that require criminal defendants to divulge encryption pass phrases in certain circumstances. In

these countries, failure to do so can lead to fines or even imprisonment.⁴

p. 57

The IRS has published new procedures under which informants may claim rewards of up to 30% of additional tax, penalties and interest owed. To be eligible for an award under the new procedures, the tax, penalties, interest, additions to tax, and additional amounts in dispute must exceed \$2 million for any taxable year.

p. 61

The Small Business and Work Opportunity Act of 2007 imposes much higher penalties on tax return preparers that fail to meet dramatically higher standards of legal authority.⁵

p. 109

In October, 2007, legislation increasing civil and criminal penalties for violations of the International Emergency Economic Powers Act (IEEPA) came into effect. Civil penalties increase from \$50,000 to \$250,000 per violation, or twice the amount of the violating transaction. Criminal penalties increased to \$1 million per violation. Prison terms of up to 20 years remained unchanged.

p. 123

A cross cut shredder is probably sufficient to protect you against a dumpster-diving identity thief. But it may not deter a more determined snoop. Researchers have developed software that can reassemble shredded documents, in some cases, with nearly 100% accuracy. If you really want to make sure that a document is unreadable, burn it, then stir the ashes.⁶

p. 140

Germany's top police official claims that German police are unable to decipher the encryption used in the Skype Internet telephone service to monitor calls by suspected criminals and terrorists.⁷ Perhaps to better deal with this situation, Germany is developing "remote forensic software" to monitor Skype conversations.⁸ There is no reason to believe that police in other countries aren't already using such software. Nor

is there any assurance that German police—or skilled hackers—aren't able to decrypt Skype communications.

p. 142

Hushmail (<http://www.hushmail.com>) now acknowledges that the company will eavesdrop on its users when presented with a valid court order. In June 2007, Hushmail provided 12 CDs of emails to U.S. officials targeting steroid manufacturers, in response to a Canadian court order.⁹

p. 157

The Tax Relief and Health Care Act of 2006 increased the penalty for filing a "frivolous" tax return from US\$500 to US\$5,000. Some examples of frivolous returns include: failing to sign the return; taking the position that the Constitution forbids imposition of a federal income tax; or filing a tax return with zeros entered on every line, even though you have taxable income.

pp. 243-244

A proposed change in the tax treatment of U.S.-based captive insurance would eliminate their ability to claim tax deductions for money set aside in reserves to pay for future claims and losses. If this proposal comes into effect, it will greatly increase the attraction of non-U.S. captive insurance companies.¹⁰

pp. 249-250

Proposals now before the U.K. Parliament would increase tax charges for non-domiciled residents. Persons living or working in the United Kingdom, but domiciled elsewhere, would be required to pay an annual £30,000 charge after seven out of ten years residence and a higher rate of £50,000 after ten years. These charges could be avoided by becoming non-resident, or by electing to be taxed as a domiciled U.K. resident.¹¹

Notes

¹ "U.K. Government Says no Plans for FBI DNA Database Hookup." *The Register*, Jan. 17, 2008.

² "New Backdoors for U.S. Secret Service Found at U.S. Telcos." *Heise-Security News*, Dec. 17, 2007.

³ "Cellphone Tracking Powers on Request." *The Washington Post*, Nov 23, 2007.

⁴ "Man Can't be Forced to Divulge Encryption Passphrase." *News.com*, Dec. 14, 2007.

⁵ *The Jacobs Report*, Jan. 9, 2008.

⁶ "Computers to Reassemble Shredded East German Secret Police Files." *Fox News*, May 10, 2007.

⁷ "Skype Encryption Stumps German Police." *Yahoo! News*, Nov. 22, 2007.

⁸ "Skype Trojan Wiretap Plans Leaks Onto the Net." *The Register (U.K.)*, Jan. 29, 2008.

⁹ "Hushmail To Warn Users of Law Enforcement Backdoor." *Wired Blog*, Nov. 19, 2007.

¹⁰ "U.S. Tax Plan Could Drive Captive Insurers Offshore." *Reuters*, Jan. 29, 2008.

¹¹ "Non-Dom Tax Moves 'Will Drive Rich Away.'" *The Telegraph (U.K.)*, Jan. 22, 2008.