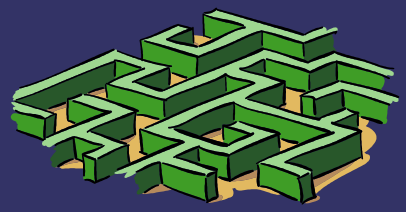
How to Survive a Federal Investigation

Paul Timmins

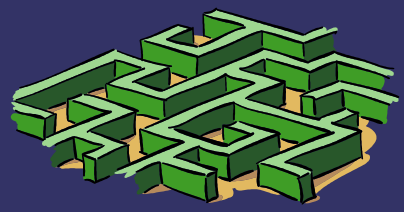
This presentation is not legal advice, I am not an attorney (yet). (Yes, I'm working on it)

If you ever need to know this, FOR THE LOVE OF GOD RETAIN ONE!



Overview

- Nobody in the Government knows what's going on.
- There are a few FBI Agents who know what they are doing w.r.t Computers, but the majority do not, or do not know much about it.
- It is the intention of the prosecutor that you never see your day in court.
- The Government does not have the resources to properly prosecute a computer crime.



Examples of government incompetence

UNITED STATES OF AMERICA

V.

WARRANT FOR ARREST

PAUL G. TIMMONS

CASE NUMBER: 5:03cr53-3-

The United States Marshal
and any Authorized United States Officer

YOU ARE HEREBY COMMANDED to arrest **PAUL G. TIMMONS**
Name

and bring him or her forthwith to the nearest magistrate to answer a(n)

[X] Indictment [ ] Information [ ] Complaint [ ] Order of court

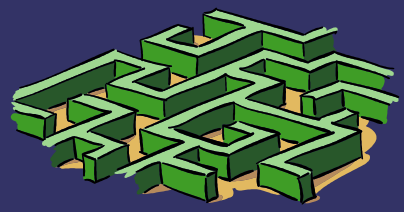
[ ] Violation Notice [ ] Probation Violation Petition

charging him or her with (brief description of offense)

Possession with intent to distribute and importation of cocaine.

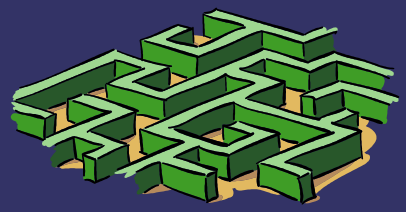
in violation of Title 18 United States Code, Section(s) 2, 371, 1029, 1030, 1343

Importation of Cocaine?
Paul Timmons? Can they at least spell the name right on the arrest warrant?



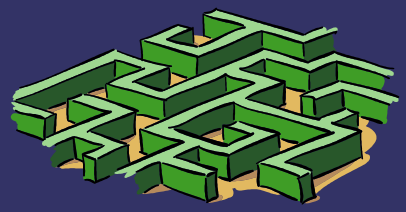
The Indictment

- Grand Jury Indictments are secret.
- You do not get to know one is happening.
- You do not get a chance to fight it before it happens.
- You do not get to know what the jury was shown.
- Once you are indicted, you do NOT get a preliminary hearing. You're stuck going to trial, or pleading out.



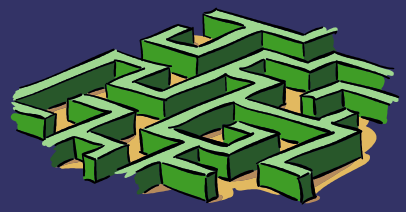
Plea Bargains

- What? Yes. Plea bargains.
- A product of the expense of a proper defense.
- I was arrested in November of 2003. I was sentenced in April 2005 (2 days before NAC 2!). In that time I moved, went through two cars. How much life would I have lost to this case if I took it to trial? I plead!



There is such a thing as a federal misdemeanor!

- You have no idea how hard it is to explain this concept. I actually had to show the cashier paperwork at the court that said MISDEMEANOR on it before she believed me.
- She then called over her coworkers “Y'all, come look at this!”
- She then had to call helpdesk to figure out how to ring up a misdemeanor fine. She has never rang up one before.



DOOM!

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
STATESVILLE DIVISION

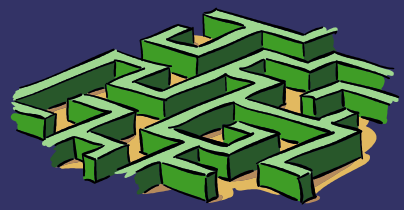
NOV 19 2003

U. S. DISTRICT COURT
W. DIST. OF N. C.

UNITED STATES OF AMERICA	)	DOCKET NO. 5:03cr53-MCK
	)	
	)	BILL OF INDICTMENT
vs.	)	
	)	Violations:
	)	18 U.S.C. § 2
(1) BRIAN A. SALCEDO,	)	18 U.S.C. § 371
(2) ADAM W. BOTBYL a/k/a "itszer0", and	)	18 U.S.C. § 1029
(3) PAUL G. TIMMINS a/k/a "nowcb4u"	)	18 U.S.C. § 1030
	)	18 U.S.C. § 1343

THE GRAND JURY CHARGES:

At the specified times and at all relevant times:



GRAB ANYTHING PLUGGED INTO THE WALL

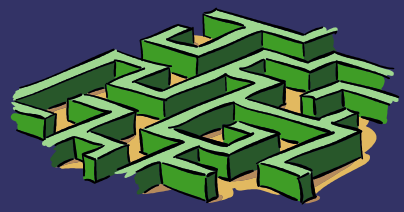
How the federal government executes a computer search warrant.

Things they tried to take but didn't: (Thanks Becky!)

- ✗My cable box
- ✗My dreamcast

What they did take:

All my dreamcast games.
An AIX machine without a hard disk.
A 386 in several pieces.
Random motherboards.
A homebrew 48v power supply that was basically a transformer in some sort of homebrew enclosure.
I didn't dare touch that supply myself. OMG DANGER!



“Hey, they're talking about you on NPR!”

Newswires, TV News syndication, Internets, and follow the bodies, Oh my!

Western Europe, and parts of Asia. The rapidly spreading Wi-Fi provides speedy Web links on the go. And wireless companies are rolling out ever-faster ways for their customers to tap the Net. On Jan. 8, for instance, U. S. giant Verizon Communications Inc. is expected to unveil a nationwide rollout of a competing wireless technology that provides data speeds of up to two megabits per second.

Even if incumbent telecom companies hold back, rivals are likely to see opportunity in WiMax. The No. 5 mobile operator in the U.S., Nextel Communications Inc., has been snapping up broadband wireless licenses around the country and is widely expected to enter the business. Digital subscriber line (DSL) providers such as Covad Communications Group Inc. also could jump on WiMax to free themselves from the cost of licensing phone lines from regional Bell operating companies. And a crop of so-called wireless Internet service providers that offer local Wi-Fi services are prime candidates to graduate to WiMax.

Perhaps the biggest opportunity for WiMax lies in the developing world. Large areas of Latin America, Asia, Africa, and Eastern Europe aren't wired for telephone service, let alone cable. With WiMax, they could leapfrog directly to broadband. That's one reason players such as China Unicom Ltd. and Serbia's Telekom Srbija are already rolling out broadband wireless gear. These and dozens of other companies likely will switch to even cheaper WiMax when it becomes available. Pyramid Research figures that the number of broadband wireless users in the developing world will grow at a compound annual rate of 54% over the next five years, vs. 34% in developed nations. "WiMax could help close the Digital Divide," says Pyramid analyst John Yunker.

Suppliers already are scrambling to serve the market. "We are big believers in broadband wireless," says Niel Ransom, chief technology officer for Paris-based Alcatel, the world's No. 1 seller of conventional DSL gear. Alcatel hasn't announced WiMax products yet, but "there's no way we're going to sit on our hands," Ransom says. Neither is Alvarion, which is likely to be the first company to release WiMax-compatible gear late this year. All told, figures Pyramid, operators will spend $8.4 billion over the next four years on broadband wireless gear.

For consumers, WiMax holds out the promise of increased broadband competition, lower prices, and more freedom. That's a combination sure to turn a few heads. ■

–By Andy Reinhardt in Paris

SECURITY

For Now, Wi-Fi Is A Hacker's Delight

You've heard of a drive-by shooting, but maybe not drive-by hacking. It's a worrisome sort of cybercrime in which burglars sit in a car outside a company and use laptop computers with antennas to hack into cash registers and corporate records by snagging data as they travel over the airwaves. That's how two men allegedly snatched the credit-card numbers of customers of a Lowe's Home Improvement store in Southfield, Mich., recently. Another mobile thief pleaded guilty just before the holidays to hacking into patient records at Wake Internal Medicine Consultants Inc. in Raleigh, N.C.—just to show how vulnerable such records are to hackers.

Plugging Wi-Fi's Gaps

How to keep hackers out of corporate wireless networks:

- Install the latest encryption software, called Wi-Fi Protected Access
- Set up an "invite list" specifying which machines can connect to the network
- Build a "virtual private network," a secure pathway protected by passwords

It happens all the time, according to network security experts. Thanks to the booming popularity of Wi-Fi networks—which let untethered laptop users gain access to the Net from the living room, the airport lounge, or a parked car—keeping such networks secure has become one of the technology industry's biggest problems.

The players who make wireless equipment are racing to limit the potential for damage. Improved security standards should be ratified later this year by the association that sets tech industry standards, the Institute of Electrical & Electronics Engineers (IEEE). By mid-2004, Wi-Fi component makers such as Intel Corp. and Cisco Systems Inc. will release products with the emerging standards. In the interim, the nation's biggest operator of public Wi-Fi networks, T-Mobile HotSpot, plans to deadbolt its systems with upgraded encryption. "Security is of paramount concern to everybody," says Joe D. Sims, general manager of T-Mobile HotSpot.

The new security standards will help, although they won't plug all of Wi-Fi's security gaps. Security keys will be changed every time data are transmitted, instead of staying the same throughout a Wi-Fi session. And the encryption of data will be beefed up from the old 64 kilobits to 256 and will use next-generation cryptography. Still, Wi-Fi networks likely will remain vulnerable to sophisticated hackers.

"There's no way you can contain the Wi-Fi signal so people can't get to it," says Paul Brock, a managing director at brokerage firm Bear, Stearns & Co.

Even these limited safeguards can't come fast enough. After beginning as a grassroots movement among home PC users, Wi-Fi was brought into the office by workers who didn't want to be anchored to their desks. Almost a third of U.S. companies either used Wi-Fi or conducted pilot programs last year, according to Boston researcher Yankee Group. An additional 14% plans to implement the technology in 2004. The concern is that these corporate Wi-Fi networks—sometimes installed by eager techies without the knowledge of the IT department—have exposed companies to outside thieves. "They punch a huge hole in the corporate security system," says Pankaj Manglik, founder of wireless security firm Aruba Wireless Networks Inc.

Even before the new security standards come out, businesses and individuals can help protect themselves. Any Wi-Fi system comes with built-in encryption, called WEP, for wired equivalent privacy. But it must be turned on, and many users neglect to do so. Still, WEP encryption is weak. A determined hacker can unscramble key passwords in hours, if not minutes. "Break-ins are as common as breathing," says Bruce Schneier, founder of Counterpane Internet Security Inc. For the wireless future to get safer, it's a good policy to keep as many padlocks on corporate airwaves as possible.

–By Roger O. Crockett in Chicago

Photos by Max Ortiz / The Detroit News

Mike Klein, president and CEO of Interlink Networks in Ann Arbor, shows how wireless networks, or Wi-Fi work. The company specializes in wireless and wired computer security.

New wireless networks spark security concerns

Businesses fear hackers but few use protections

By Charles E. Ramirez
The Detroit News

Businesses have been moving to wireless technology, but many fail to use security software, such as Interlink's.

A couple of months ago, police caught three cyberthieves trying to hack into the wireless computer network at a Lowe's home improvement store in Southfield.

The trio, which allegedly tried to access the retailer's national computer system to steal credit card information, faces 16 federal criminal charges in North Carolina, where Lowe's has headquarters.

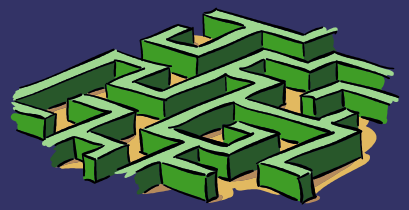
While the theft was foiled, the episode laid bare the growing threat that tech-savvy crooks pose to businesses, particularly as wireless technology becomes more popular. Analysts say many companies fail to take the necessary security steps to protect themselves and the vital data inside their computers: business plans, intellectual property, financial statements and personal data from customers and employees.

Last year, 251 U.S. companies reported losing $202 million because of cybercrime, according to a survey conducted by the San Francisco-based Computer Security Institute and the Federal Bureau of Investigations. The survey also found $70 million of that total and the greatest financial loss was tied to the theft of proprietary information.

"The security issue is real and for businesses its got to be rule No. 1," said Mike Klein, president and CEO of Interlink Networks, a wireless and wired computer network security software company based in Ann Arbor.

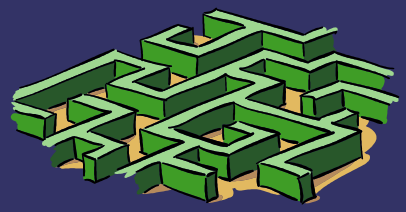
Security concerns are especially pressing as more and more companies turn to Wi-Fi technology, which lets users link computers and other devices via high-frequency radio waves instead of with cables and wires.

Please see SECURITY, Page 7B



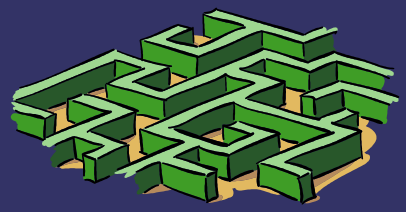
Where I was mentioned

- Every morning drive radio show in Detroit
- NPR
- The 6pm edition of Fox 2 news. The opening shot was at the Southfield Lowes. I saw that and thought one thing: “DOOMED”.
- Page 1 of the Oakland section of the Detroit Free Press, in larger print than “Teen Killers Sentenced”.



Just when you think it's over

- I was released from probation just after thanksgiving of 2005. I have no gun restrictions, or any ongoing restrictions, and a class a misdemeanor on my record.
- You'd be surprised how many systems run under the assumption that any federal crime is a felony.



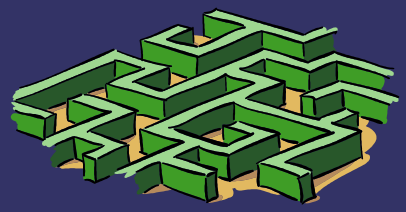
NICS

The National Instant Criminal Check System (used for firearms checks)

NICS can return 3 types of response -

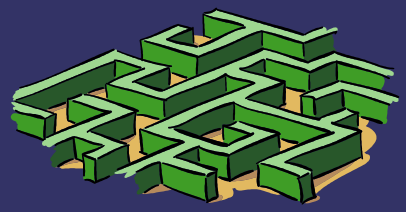
1. Proceed (you can have the gun)
2. Decline (no gun)
3. Delay (they will defer the results for further investigation)

I've been run in NICS 2 times. Each time, I was returned a delay. In the event of a delay, NICS has 72 business hours (3 business days) to return a response. At that point, at the FFL's discretion, they may tender the firearm. Dunhams has a corporate policy not to. Fortunately, that's not the case with most FFLs. :)



“So you're a computer hacker, eh?”

- Police MDTs generally have access to your criminal record. Inevitably, you'll always hear about it when they're giving you crap.



“At least when I die, I'll be remembered for something”

- Google knows me. It knows me well.
- Stupid webloggers who don't do their homework have attached my name to things that are either factually inaccurate, or bordering on slanderous.
- As you can imagine, it makes sending resumes a dicey proposition :)