

http://www.toad.com/gnu/ Go JUL AUG SEP 14 2016 2017 2019 630 captures 1 Mar 2000 - 25 Jan 2021 About this capture

John Gilmore, Entrepreneur and Civil Libertarian



**I'M STILL FREE.
WHAT ABOUT YOU?**



[Why I'm Not Answering Your Email](#)

[US Homeland Security recorded what book I was reading as I crossed the border](#)

In direct violation of the Privacy Act, which states that federal agencies shall not record the how citizens use their First Amendment rights (unless specifically instructed to do so by statute), the US Department of Homeland Security recorded in my permanent dossier that as I flew into San Francisco from London, I had **"many small flashlights with pot leaves on them. He had a book entitled 'Drugs And Your Rights'.** [sic]" Images of the flashlight and the book are above.

The Gestapo cared what works of philosophy you were reading. So did the Stasi. Those of you who live in free countries may find it a bit hard to understand why any populace wouldn't tear to bits any bureaucrats that would take away the fundamental right to read whatever you like without it being used to determine how your government treats you as you cross borders or travel within your own country.

http://www.toad.com/gnu/ Go JUL AUG SEP 14 2016 2017 2019 About this capture

630 captures 1 Mar 2000 - 25 Jan 2021

The United States is not a free country. Only when the DHS is dissolved, disbanded, disempowered, and disrespected will there be any prayer of freedom.

Those of you in free countries may like to read [the book that DHS found so interesting](#), or meet the [Rutgers professor of philosophy, Douglas Husak](#) who wrote it. You may even want to carry a small, useful keychain flashlight advocating for "Freedom of Thought". [Freedom of thought](#) needs more advocates.

Current Projects

[Freedom Boxes](#). [Eben Moglen](#) created the Freedom Box Foundation to create and spread tiny, cheap home servers that use free software to provide freedom and privacy for individuals. These compete with "cloud-based" services that put your privacy and your freedom under the control of third parties who don't have your interest at heart. These boxes are designed to make mass surveillance impractical and thus to safeguard political liberty (even in countries that don't favor individual liberty). See the [video](#) or [transcript](#) of Eben's speech on "Why Political Liberty Depends on Software Freedom More Than Ever". I'm helping.

[A Shade Structure for Burning Man](#). I built a pretty simple shade structure for our camp at the Burning Man festival.

[Freedom of Movement / Secret Law](#). I sued [TSA](#) to make them stop demanding that citizens identify themselves in order to travel. Not only airports, but trains, cruise ships, and some buses, are now "asking for" IDs. You can't read the rules -- they define your rights and obligations, but they're super secret information (SSI). I petitioned the US Supreme Court to examine whether the Feds can enforce secret regulations. **I lost every one of these lawsuits. The Constitution is a dead letter as far as the one-branch Federal dictatorship is concerned. Whatever the Executive does, Congress and the courts rubber-stamp.** What we did discover is that there is no requirement to show ID to get on an airplane. TSA said so in their papers and in open court. But each of these courts refused to make TSA stop lying to the public with airport signs telling every passenger that their ID is "required".

If you politely decline to show ID whenever someone asks (or demands) it, and continue politely declining regardless of how they escalate, you will discover what your rights are. You'll be surprised. You'll get away with it. Most of the people who were asking for it have no right to demand it. They've been relying on your voluntary cooperation. They forgot to tell you that part; but you just found it out for yourself. Sometimes you may discover that you didn't have the right to live, move around, or do business in your own country without government-issued documents. That's very interesting knowledge to acquire first-hand too. If you haven't recently tried exercising your right to exist and live without government permission, are you sure you still have that right?



[Deflating Idiocy About Security](#). The US government says we are always at an "Elevated" threat level. They have no plans to ever reduce this reported threat level down to "Low", no matter how many years of untroubled life we go through. It's like the Bulletin of the Atomic Scientists' "doomsday clock" which in over fifty years has never been shown with less than 17 minutes remaining before Armageddon. Well, 17 minutes have ticked past more than a million and a half times since 1947, and the bombs haven't blown us up. These are both scare tactics, not real reflections of reality.

In reality, the likelihood of you being directly affected by a terrorist attack has not gone up or down since 9/11; the likelihood has always been extremely low. You and your friends are far more likely to die in bed, in

http://www.toad.com/gnu/ Go JUL AUG SEP 14 2016 2017 2019

630 captures 1 Mar 2000 - 25 Jan 2021

Similarly, as you ask for your friends being directly affected by an atomic explosion is also less than 1000 captures at 10AM rather than 10PM

About this capture

[Disarming the rogue United States](#). The United States should be forced by United Nations resolutions to surrender its "weapons of mass destruction" or face the consequences. "That nation has gone beyond the pale. It repeatedly threatens and attacks other sovereign countries without provocation, holds massive stocks of nuclear and conventional weapons, tortures its own citizens and those of other countries, refuses to follow its own constitution and laws, breaks international treaties which it co-created and signed, holds 500,000 political prisoners in its jails. It imprisons the largest number and percentage of its people in the world. Every government with that kind of track record needs to immediately disarm and submit to a regime change, or face the consequences from the international community."

[What's Wrong with Copy Protection?](#) Why should self-interested companies be permitted to shift the balance of fundamental liberties, risking free expression, free markets, scientific progress, consumer rights, societal stability, and the end of physical and informational want? Because somebody might be able to steal a song? That seems a rather flimsy excuse. This early paper on DRM (Digital Rights Management) systems is still relevant in spots.

Things I've Started

The [Electronic Frontier Foundation](#) (with Mitch Kapor, John Perry Barlow, and Steve Wozniak)

A foundation dedicated to civil rights and civic responsibilities online. Here's a few [documents](#) I made with EFF. Here is a speech on [Privacy, Technology and the Open Society](#) that I gave at the First Conference on Computers, Freedom and Privacy. I'm still quite active in EFF, and serve on its Board of Directors.

The [Cypherpunks](#) (with Eric Hughes and Tim May)

An informal group dedicated to public education and dissemination of encryption (also known as cryptography, the science and art of secret writing). I originally hosted the mailing list (cypherpunks@toad.com) and provided space for the first few years' worth of meetings. A descendant of the mailing list is still operating; subscribe to cypherpunks@metzdowd.com.

The "[alt](#)" newsgroups on the Usenet (with Brian Reid and Gordon Moffett)

A forum for discussions that the ``mainstream" Usenet refused to handle, like sex, drugs, and gourmet cooking. I supported nationwide (US) links among the original ``alt" sites until it became popular enough that almost everyone carried it. I set the original newsgroup creation policy in ``alt", which was to ``Use common sense." Alt has flourished as a haven for popular and unpopular topics, and was targeted by CompuServe for censorship in December 1995 because they felt that some of the free speech in it was too free for them to handle. The alt groups are self-regulating (or self-unregulating) and I have not been involved in alt policy or group creation in many years.

[Cygnus Solutions](#) (with Mike Tiemann and David Henkel-Wallace)

A company that provides commercial support for free software. They support the GNU programming software (from the [Free Software Foundation](#)), I co-managed the company, provided engineering leadership, was the official maintainer of GDB for several years and led the GDB programming team, supported numerous customers, and led the Cygnus Network Security (Kerberos) product team. I instituted a culture of distributed hiring, automated software testing, and frequent software releases across scores of platforms, much of which persists to this day. I stopped working daily at Cygnus in April 1995, and left the Board of Directors in January, 1997. The company was bought by [Red Hat, Inc](#) in November, 1999, for \$675 million. They're still doing fine as a big piece of Red Hat.

I've scanned in some [Cygnus marketing materials](#) showing some of the early evolution of the free software market.

[The Little Garden](#) (with John Romkey, David Henkel-Wallace, and Steve Crocker)

A medium-sized Internet Service Provider in the San Francisco Bay Area. now merged into Verio. We mostly sold T1 and 56K Internet connections to businesses. We were distinguished from many other

http://www.toad.com/gnu/ Go JUL AUG SEP 14 2016 2017 2019 630 captures 1 Mar 2000 - 25 Jan 2021 About this capture

service at lower prices. TLGnet was sold to [Best Internet Communications](#) in July, 1996, and my active involvement in it ended. (Best was then bought by [Hiway Technologies](#), which was then bought by [Verio](#).)

[GNU Radio](#) (with Eric Blossom)

A software project that decodes and encodes radio and audio signals in software. It's a specific example of "Digital Signal Processing", but designed to be good at handling high speed (or wideband) signals. It's free software.

GNU Radio can receive and decode over-the-air HDTV signals in the US standard "ATSC" format. This decoder enables researchers to demonstrate a full software implementation of the ATSC format, and also provides a reference implementation for other designers. The decoder software currently (May 2003) runs about 40x slower than realtime, but enables the realtime recording, slow decoding, and later full-speed playback of HDTV signals. I have verified that the software works, on my own equipment. Here are example [images #1](#) and [#2](#) decoded on May 13, 2003 from KQED-DT, channel 30 in San Francisco, California.

In 2008 I catalyzed [Kestrel Signal Processing's](#) donation of the OpenBTS cellphone base-station software to the Free Software Foundation as part of GNU Radio. In 2009 I wrote and contributed smqueue, an SMS text message queueing and delivery module, to that part of GNU Radio.

[Gnash](#), the GNU Flash player (with Rob Savoye)

No working free software or open source flash player existed to display the average web page that contains embedded Macromedia Flash objects. Richard Stallman therefore made such a player a high priority project for the Free Software Foundation.

I knew [Rob Savoye](#) from Cygnus, and knew he'd done some work on an embedded Flash player, so I asked if I could pay him for six months to turn that open source embedded Flash player into a GNU flash player. He agreed, and the Gnash project was born. It currently provides a standalone player which builds and runs on a variety of systems, using OpenGL and other renderers, plus a browser plugin. The project is now financially supported by a commercial company, Lulu.com, which stands to benefit from its rapid evolution. It is now able to play Flash videos from [YouTube](#) and [Lulu.tv](#). Stay tuned; a solid community of contributors are improving it daily.

Things I've Put A Lot of Energy Into

[Sun Microsystems](#)

Sun is a computer manufacturer, long a leader in the technical workstation and database markets. Many Web pages are served from a Sun server. Sun is now a multi-billion-dollar company; working there made me financially independent. It was acquired by Oracle in 2010. I was its fifth employee, and later a consultant. I handled architecture, design, implementation, and debugging of Sun Workstations. Wrote and maintained bootstrap and diagnostic ROMs for the Sun-1, Sun-2, and Sun-3. Debugged first prototypes of Sun-1 and Sun-2, working with the hardware designer. Worked on first bringup ever of Unix on Motorola 68010 and 68020. Designed and diagnosed the chip designs for the SPARCstation-1 and SPARCstation-2. Straddled the hardware and software camps to locate, explain, and solve design, implementation, and manufacturing problems. Pulled many chestnuts out of fires. Debugged Unix utilities, kernel, device drivers, and CAD software. Diagnostics. Documentation. Electronic mail maintenance, support, and enhancement. Performance and code generation improvement. General technical support. Network relations. Contributed to lively corporate culture.

[Free Software](#)

Free Software means software that comes with freedom -- not software that has a price of 0. In particular, it means software that gives everyone the source code (what programmers need to keep a program running and improve on it) and the right to use the program, modify it, and give or sell copies

http://www.toad.com/gnu/ Go JUL AUG SEP Software for
 630 captures
 1 Mar 2000 - 25 Jan 2021 2016 2017 2019 About this capture

came with source code and the right to copy and modify it. This gradually changed as software became more independent from hardware. Richard Stallman realized the loss to the industry from the change, and formalized the issue with the [GNU General Public License](#) and his project to re-implement Unix freely in 1983.

I ported Richard's GNU Emacs to the Sun Workstation that year. I started archiving the free software posted to the Usenet in 1981, and continued through 1987 or so. I started a project to "sift the sands of Berkeley Unix", collaborating with UCB and other Unix hackers to sort the nuggets of original, nonproprietary code out from the background of AT&T-licensed code. Ultimately this resulted in the Berkeley "Networking 2" release, which didn't require the recipient to have an AT&T license. In 1985 I wrote the "pdtar" program, which eventually became [GNU Tar](#). In 1986 I tested pre-releases and each public release of the [GNU C Compiler](#) (now called the GNU Compiler Collection). I wrote GNU UUCP and hacked on the GNU Debugger and GNU Make in 1988 and 89. I ported most of Berkeley Unix through GCC in 1989 for UC Berkeley, so they could abandon the proprietary AT&T C compiler, as part of the effort to make BSD Unix freely available. In 1989 I co-founded Cygnus Support, the first company dedicated to supporting free software. Cygnus has made major contributions to free software, including better documentation, quality assurance, cross-compilation, many ports to new hardware and operating systems, and marketing help to get free software accepted by the computing mainstream. While at Cygnus I maintained the [GNU Debugger \(GDB\)](#) from 1990 through 1993. I worked on MIT's free Kerberos software for Cygnus from 1994 through 1995. I served on the Program Committee for the First Conference on Freely Redistributable Software in February 1996. Throughout 1996 I worked on securing the Berkeley Internet Name Daemon ("BIND"), the free software which holds the Internet together by mapping domain names to and from numeric Internet addresses, using [Domain Name System Security \("dnssec"\)](#).

From 1996-2003 I co-created and sponsored [FreeS/WAN](#), which added IPSEC (cryptographic security and privacy) to Linux's Internet networking support. In 2001 I co-created and sponsored [GNU Radio](#), a framework for digital signal processing of radio-frequency signals. In 2005 I co-founded [GNU Gnash](#) with [Rob Savoye](#) (who is doing all the work). In 2007, [Don Hopkins](#) and I convinced [Electronic Arts](#) to release Will Wright's original groundbreaking [SimCity game](#) (which started the billion-dollar Maxis/EA "Sim" series of games), released for free to the children of the world under the GNU General Public License (v3) as "Micropolis" (its original code-name). I also helped the [One Laptop Per Child](#) project with quality assurance, writing and editing, tech support, and other collaboration. In 2009 I wrote smqueue, a queueing and delivery system for [SIP-based text messaging](#), which processes SMS messages for cellphones handled by [OpenBTS](#) GSM cellphone base-station software (which is part of GNU Radio). I still contribute occasional changes to various free software program.

Freedom of Information

I have put a lot of time and money into researching what the government is doing, using Freedom of Information Act (FOIA) requests. I have sued the US Government several times to enforce the FOIA against agencies who have little or no interest in letting the public know, in a timely fashion, what they have been doing to or for us.

In 2006 I sued the government to demand that it either publish the secret law that requires citizens to show ID in order to travel in the United States -- or to stop enforcing that secret law. This is part of my [Freedom to Travel](#) case. The FOIA does not apply to this secret law, because Congress specifically exempted airline security directives from the FOIA. Congress could not exempt them from the Constitution, which requires that citizens be given notice of what the law requires -- but the courts did exempt them from it, by refusing my case every step of the way.

Encryption Policy

Encryption is secret writing. Codes and ciphers. Spies. Encryption was originally used by military and diplomatic organizations; Julius Caesar invented an encryption scheme. In the last century, electronic communication (telegraphy and radio) made it widely useful, and computerization has made it

http://www.toad.com/gnu/ JUL AUG SEP for everyone
 putting "envelopes" around your email for privacy, moving money around the Internet safely, to protect
 630 captures you're really you when you're halfway around the world. 14 2016 2017 2019
 1 Mar 2000 - 25 Jan 2021 About this capture

The US government is deathly afraid of its own citizens (and non-US-citizens) having access to good encryption. This fear extends all the way up to the Vice President and the head of the FBI, who personally get involved in creating encryption policy. Everyone in government refuses to tell us why, saying it's classified and the national security is at stake. Rubbish! The security of the nation is already gone when its government violates the basic rights of its own citizenry, as these agencies do every day. They are "burning the Constitution in order to save it". (My own belief is that what's really at stake is a wiretap-based power base that J. Edgar Hoover and the classified spy agencies have built up for their own benefit.)

The most Byzantine set of laws, regulations, policies, departments, and practices you've ever heard of are employed by the National Security Agency and three or four other Executive Branch departments in an attempt to keep good crypto from bad guys. Unfortunately, they have also succeeded in keeping good crypto from good guys who have constitutional rights. I instigated a [lawsuit](#) to correct this, with Dan Bernstein as plaintiff and the Electronic Frontier Foundation backing him up. I was a technical advisor to the lawyers in the case. On December 6, 1996, Judge Patel decided that the export regulations are unconstitutional. The government appealed, and on May 6, 1999, the 9th Circuit Court of Appeals [agreed](#) with her. The government appealed to an 11-judge panel in the 9th Circuit (an "en banc review"), which was granted, and then the government "voluntarily" changed the encryption export regulations so that most free software and academic research, and a lot of proprietary encryption software as well, can be easily published from the US. The "en banc review" of the old regulations became moot, and the case has been handed back down to Judge Patel, who ultimately ended it. The new regulations are even more complex than the old ones, and carry the same old harsh penalties for inadvertent violation. They need to not just be "reformed" but scrapped.

The government claims to retain the right to change those rules whenever it wants, and restrict encryption software again if it chooses. Congressman Judd Gregg announced support for doing so in the week of hysterical reaction after the World Trade Center was destroyed by hijacked airliners, but was shouted down by the people who'd spent a decade fighting this battle before he could gather any political support.

I have had an interest in encryption since childhood, and have spent a lot of time working on [crypto export control issues](#).




I led the team that built the world's first publicly announced [DES Cracker](#), a machine that finds the secret key used to encrypt messages in the government's favorite encryption scheme, the Data Encryption Standard (DES). The National Security Agency intervened when the scheme was being standardized in the early 1970s, shortening the secret keys so that they could build their own DES Crackers. But they spent the next 25 years lying to us about how secure the scheme is, to encourage everyone to use it -- and we did. This left NSA able to secretly eavesdrop on anyone who used DES, which includes the entire financial community, and most computer and network security systems. Technology has advanced to where anyone with \$200,000 can break the code, leaving all of our DES-protected infrastructures at risk. [Thanks NSA!](#) By 2010 much of the older DES-based software has been replaced, though there are a few places that still use it, and its use is still an option in some protocol implementations even though it is known to be insecure. NIST has standardized a new algorithm with much longer keys, which has not been studied nearly as long as DES, but which has resisted all attacks so far. Smart people long ago stopped designing DES into new systems. Triple-DES or AES seem to be the preferred replacements.

Securing the Internet

As I say below, my [FreeS/WAN project](#) is to secure Internet traffic against wiretapping.

Drug Policy Reform

(See my [Drug Policy Reform](#) page.)

http://www.toad.com/gnu/ JUL AUG SEP 14 2016 2017 2019   

more than 2,500,000 people in prison in the United States -- supposed
 630 captures One quarter of the world prison population is imprisoned in the
 1 Mar 2000 - 25 Jan 2021

are imprisoned at large multiples of their actual incidence of criminal behavior.

[458,000 of those people](#) were in prison for non-violent mind-altering drug charges in 2000; [about 500,000](#) in 2008. The federal [Bureau of Justice Statistics](#) reported 155,900 in city or county jails for drug offenses (2002); 251,400 in state prisons (2008); and 95,205 in federal prison (2009). Don't forget the additional 582,759 nonviolent drug users on probation and the 261,666 on parole in 2009. By 2012, about 210,200 were in state prisons; in 2013, 98,200 in federal prison, plus [986,000 on probation and 268,656 on parole](#). I have no recent data on state jail populations from drug arrests, except in scattered states. More than half of all federal prisoners are imprisoned for drug crimes.

Many of these political prisoners are otherwise law-abiding people, making families and pulling their weight in society. The vast majority of them are black or Hispanic. The policy that locks all of them up, and makes their drug-using friends fear their own government, is [wicked and racist](#). It damages our citizens' respect for the law, it encourages corruption in our government institutions, it has been responsible for major losses of our constitutional rights, and has wasted hundreds of billions of taxpayer dollars. It has also cost millions of people their time and money to fight the criminal justice system. It encourages violent resolution of commercial disputes with drug sellers, by denying recourse to courts, harming not only those people but their families, neighborhoods, and innocent bystanders. The US has forced this policy down the throats of countries all over the Earth, vastly multiplying the misery and injustice it creates. And it artificially raises the prices of these substances, feeding our citizens' money to many violent and irresponsible suppliers. At least [68 million people](#) have used illegal drugs (as of 1996), including our own [Presidents](#), but the madness persists. The obvious lies that the government tells in furthering its drug policy make every thinking citizen doubt other statements -- even true ones -- from such an obviously corrupt government.

Besides the practical issues, there are fundamental rights involved. The right to speak freely is irrelevant if the citizenry does not have the right to think freely. Our government's control of drugs is really intended to control our citizens' mental states. The substances themselves are not important unless they affect human minds (and some, such as nitrous oxide, are freely sold for non-mind-altering uses, but controlled when people wish to influence their own mental states).

These drugs appear to be prohibited by the government because they permit users to see that the world is not composed of a single point of view, a single concrete reality shared by all. The way each of us interacts with the world is a function of our internal brain chemistry, which is unique to each of us, and can be altered by our own choice or by imposed choices. The government seeks to impose **its** answer to the choice of whether or not to view reality in certain ways. These altered ways have clearly been useful in religion, art, music, medicine, and recreation for millennia. These government attempts to control the minds of its citizens are a direct violation of the basic constitutional freedoms that the government is designed to secure for ourselves and our posterity.

I have known many people throughout my life who are able to **use** drugs in appropriate settings without harm to themselves or to others. I have known a few who were unable to control their use, and abused drugs. Today's policy does not "cure" these drug abusers, nor successfully remove them from society. The huge number of harmless users swept up in the gears of "justice" swamp the system, preventing the real troublesome people from being reformed or isolated.

Just as adults keep immature children away from matches and hot objects, though there is no law prohibiting the possession of matches by children, parents and social feedback should be used to teach children how to handle drugs responsibly. The War on Drugs has certainly not kept children from being able to get drugs! By eliminating the black market and the threat of prison, and allowing straightforward talk from people who know the dangers first-hand, children can learn the real reasons why some drugs are best avoided, and learn the line between use and abuse of other drugs. Today's situation teaches children that it's best to sneak and lie about what they're doing -- both because they are afraid of prosecution, and because they see drug-using parents doing the same thing.

http://www.toad.com/gnu/ Go JUL AUG SEP 14 2016 2017 2019 About this capture

630 captures
1 Mar 2000 - 25 Jan 2021

way that damages people around them (or seriously threatens to), they should be held responsible -- whether the drug is coffee, alcohol, or cocaine.

No matter who you are, you know someone who uses illegal drugs. Talk with these people about the real effects and the real dangers of the drugs they use, compare what they tell you to what the government tells you, and ask them about how the current drug laws and policies affect their life. If you think you don't know any drug users, think again of who you know. Are you really sure about all of them? If you still can't think of anyone, ask your friends in private whether they have ever used illegal drugs. You'll be surprised at what some of them have been afraid to tell you. Learn from what they know, but learn especially from the paranoia and fear they have had to live in. Then work with me for a peaceful end to the Drug War and a sane policy for how to treat our fellow citizens.

[One Laptop Per Child](#)

This project seeks to build millions of small, child-friendly laptops and get them into the hands of students in Third World countries. The laptops and software are being designed by educators with decades of experience teaching kids using computers, like Alan Kay and Seymour Papert. Their business model is to sell the computers to the education bureaucracies of countries, in place of paper textbooks. The computers will contain many textbooks, and also provide much more infrastructure for learning. The software is almost exclusively free software or open source, giving both the project and the students limitless opportunities to customise, improve, share, and understand how their systems work.

I helped around the edges with introductions, strategy, specs, testing, Secure Digital hardware, and little bits of programming. In particular, I made sure that the hardware would handle SDHC cards (larger than 2GB), and worked on understanding and clearing the software roadblocks that kept the project from reducing the power consumption of the hardware. I also got the original SimCity game released for the OLPC as "Micropolis".

Other Interests

[Don't Trust the Census](#)

40.	██████████	██████████ Rock Creek Drive, N.W.	Female	30	Single	Native	Employed	Maid - Private home
41.	██████████	██████████ Rock Creek Drive, N.W.	Female	25	Single	Native	Employed	Maid - Private home
42.	██████████	██████████ Rock Creek Drive, N.W.	Female	25	Single	Native	Employed	Maid - Private home
43.	██████████	██████████ Massachusetts Ave., N.W.	Male	55	Single	Alien	Employed	Cook - Private family

We have recently finished another decennial data-rape, also known as the Census. But you shouldn't tell the Census anything. The law says they can't release the info you provide for 99 years -- but if they want to, they just change the law. They've done it twice before. When the US Government rounded up Japanese-Americans during WW2, the "Second War Powers Act" let them use the supposedly private census data to tell the thugs where their victims lived. Homeland Security zealots extracted similar data about Muslims and Middle Easterners in 2003, under the Patriot Act. Will your innocent ancestry, profession, or hobby be the target of the next hysterical witch-hunt? By then it will be too late to un-reveal your information. **Don't help the government constrain you; always decline to give them information.** They aren't recording it for *your* benefit. [Details](#)

[The USENIX Association](#)

USENIX is "the Advanced Computing Systems Association". It started off with meetings and technical conferences for the original creators of Unix, but as those folks expanded their interests into other fields, it too has widened. I attended lots of USENIX conferences in the '80s, met many great and talented people, and learned a lot about Unix from them. I got busy in the late '80s and through the '90s, reconnected in 2000, ran for the Board of Directors on a platform of addressing the social impacts of technology, and was elected to two 2-year terms. I left the board in 2004.

[The Libertarian Party](#)

The Libertarians are a political party dedicated to small and simple government. I'm a life member. I consider the two major parties in the US to both be morally bankrupt, and largely indistinguishable from each other. Under both of them, US and state governments continue to grow in size, cost, and influence over their citizens. Both support completely indefensible policies such as the drug policies of

http://www.toad.com/gnu/ Go JUL AUG SEP 14 2016 2017 2019 About this capture

630 captures 1 Mar 2000 - 25 Jan 2021

supports Stronghold, a version of the popular Apache web server that contains strong encryption. Stronghold is a market leader among secure web servers. C2, like my own FreeS/WAN IPSEC project, develops and archives its encryption programs outside the United States, so they can be freely shipped and used worldwide. I joined the board of C2net in 1998 and served there until it was acquired by Red Hat, Inc, in 2000.

[CodeWeavers, Inc.](#)

CodeWeavers is a commercial company that's developing and supporting the free Wine software, and helping companies who have MS-Windows products port them to Unix. I started talking with them in 1998, invested in the company in 2000, and now serve on its board.

[ReQuest, Inc](#)

ReQuest makes great home stereo components that play MP3 music. I've been talking with them since 1999, and invested in the company in 2000. I'm now on the board of directors.

[The Internet Society](#)

I was a member of the Internet Society for many years. I was elected to its Board of Trustees in July 1997, for a three-year term.

Things I've Said (That People Sometimes Remember)

"The Net interprets censorship as damage and routes around it."

This was quoted in Time Magazine's December 6, 1993 article "First Nation in Cyberspace", by Philip Elmer-DeWitt. It's been reprinted hundreds or thousands of times since then, including the NY Times on January 15, 1996, Scientific American of October 2000, and CACM 39(7):13.

In its original form, it meant that the Usenet software (which moves messages around in discussion newsgroups) was resistant to censorship because, if a node drops certain messages because it doesn't like their subject, the messages find their way past that node anyway by some other route. This is also a reference to the packet-routing protocols that the Internet uses to direct packets around any broken wires or fiber connections or routers. (They don't redirect around selective censorship, but they do recover if an entire node is shut down to censor it.)

The meaning of the phrase has grown through the years. Internet users have proven it time after time, by personally and publicly replicating information that is threatened with destruction or censorship. If you now consider the Net to be not only the wires and machines, but the people and their social structures who use the machines, it is more true than ever.

"The federal government is trying to build a surveillance society. They may be doing it with the best or worst of intentions. But the job of building a surveillance database and populating it with information about us is happening largely without our awareness and without our consent."

I said this to Washington Post reporter Ellen Nakashima, and she reported it in a front-page story on September 22, 2007 as [Collecting of Details on Travelers Documented: U.S. Effort More Extensive Than Previously Known](#).

"If you're watching everybody, you're watching nobody."

The essence of "watching" or "looking" is focusing your attention. If you diffuse your attention to encompass everything, you end up missing everything. This is exactly what the US Government is doing with its police-state tactics (searching everyone who travels; fingerprinting every foreigner who is stupid enough to arrive; etc). I said this in a [message](#) to Declan McCullagh's "Politech" list in March 2003.

"Reducing the transaction costs of co-operation"

This is what free software does. When the published copyright terms of intellectual property permit anyone to modify or improve it and re-distribute it, there is no transaction cost for people to do so. When the terms disallow these things, anyone who wants to do them must negotiate with the owner.

http://www.toad.com/gnu/ Go JUL AUG SEP 14 2016 2017 2019 About this capture

630 captures 1 Mar 2000 - 25 Jan 2021

which is quite hard and expensive to duplicate in uncooperative environments.

Books are more frequently updated by their readers this way than software, because books arrive with their "source code" -- the text -- visible to and correctable by the reader. A short note back to the author suffices. The Whole Earth Catalog was regularly improved this way.

"How many of you have broken no laws this month?"

There are too many laws, and the wrong things are illegal. Drugs, sexual publications, hiring a housekeeper and not paying Social Security, jaywalking, loitering, nontraditional sex or marriage, paying someone less than a government-set wage, not wearing motorcycle helmets, owning or wearing guns, choosing your own medicines, designing or constructing your own house, owning software that can copy DVDs, exporting cryptography, driving at the same speed as the rest of the traffic; all these things should be legal. What laws have YOU broken this month?

Any country that makes every citizen a felon is heading for real trouble. We need to reform the legislative system that keeps producing too many of the wrong laws. I first said this in a [speech](#) to the First Conference on Computers, Freedom, and Privacy in 1991.

"That's the kind of society I want to build. I want a guarantee -- with physics and mathematics, not with laws -- that we can give ourselves real privacy of personal communications."

Another memorable part of my speech on [Privacy, Technology and the Open Society](#) from the First Conference on Computers, Freedom and Privacy.

"We make free software affordable."

This is the slogan on the back of the first Cygnus Support T-shirt.

"Drug prisoners are the Japanese-Americans of the War on Drugs."

In World War II, the United States imprisoned thousands of American citizens of Japanese descent, simply because of their Japanese heritage. In the drug war, the United States is currently imprisoning more than a million citizens, solely because they choose to alter their own or their customers' state of mind with physical substances.

I believe that within fifty years **we will stand shamed**, in our own opinion and in world opinion, for this travesty of justice and civil rights. We will offer recompense to our citizens unjustly deprived of their liberties due to this spasm of paranoia. Whether we can ever repair the Bill of Rights, or restore public trust in honest government, is a much harder problem.




"When the X.500 revolution comes, your name will be lined up against the wall and shot."

Some people in love with hierarchy developed a naming system for everything in the world -- including email addresses and such. It was called X.500. Unfortunately it didn't interoperate with anything we already had -- like email addresses and domain names. This didn't stop these profoundly stupid people from embedding it into HTTPS certificates and a few Internet standards that failed, like PEM (Privacy Enhanced Mail).

I made this remark in an [email message on 2/26/1993](#) to the PEM-DEV@TIS.COM mailing list, complaining that I couldn't use the PEM encryption software because the fascists who ran the naming hierarchy wouldn't give me the name I chose. I wanted a name like "O=gnu(_at_)cygnus(_dot_)com". The main objection to this sort of "easy and obvious" name is, (the quote above). That is, when the X.500 hierarchy takes over the world, "bad" names like that one won't work any more. I switched to using PGP, which didn't impose any craziness on the names people could use.

Press Mentions

Many aren't on the web, and most of the web ones aren't indexed here, but here are a few:

http://www.toad.com/gnu/ JUL AUG SEP 14 2016 2017 2019   

630 captures 1 Mar 2000 - 25 Jan 2021

- 9 February 2011: Asia Times Online's [Follow the money](#) article quotes the usual aphorism about censorship while talking about the Arabic revolution in progress.
- 8 February 2011: newswireless.net's Wendy Grossman writes on [Blackout in Egypt, or how to close the internet](#): Internet independence, or easy censorship?
- 7 February 2011: Calgary Herald: [Revolution and the Internet](#) points out that in many recent attempts at censorship, networks of people have reconnected themselves by other means.
- 4 February 2011: The Durham Region's News Advertiser says [Egyptians prove it's impossible to shut down social networks](#): "So, it's clear, even if a government shuts down social media, it cannot shut down the people's voices."
- 3 February 2011: The H (Heise Online): [Nominations open for the Free Software Awards](#) lists me among the past winners of this award.
- 26 January 2011: Business Insider's DK Matal reports in [Egypt Revolt Post-Tunisia: Is A Dam Breaking?](#) that "Despite this censorship, such is the power of distributed computing social media -- supported over multiple communication channels -- that local twitter users are currently sending tweets via mobile telephone text messages and third party software applications," thus fulfilling my old quote.
- 6 December 2010: Network World's Mark Gibbs reports that [Microsoft routes around its own COICA damage](#), wandering from reverse-engineering Microsoft's Kinect, to [COICA](#), and how censorship regimes tend to create new ways to circumvent censors.
- 6 December 2010: InfoWorld's Peter Wayner's [12 programming mistakes to avoid](#) quotes me on "Programming mistake No. 11: Closing the source".
- 2 December 2010: die Tageszeitung's "[An der elektronischen Front](#)" reports on the 20 year history of the Electronic Frontier Foundation.
- 29 October 2010: CNET News.com's Declan McCullagh: [Amid criticism, WikiLeaks shifts focus](#). "It was a humble text-only mailing list called cypherpunks, hosted by Electronic Frontier Foundation co-founder John Gilmore, that laid the philosophical foundation for WikiLeaks."
- 1 August 2010: The Manchester Guardian (UK)'s John Naughton repeats my censorship quote in [WikiLeaks: look before you leak...](#), then notes that "The aphorism came up a lot last week following publication by the Guardian, the New York Times and Der Spiegel of extensive reports based on the stash of classified US military reports published on the WikiLeaks website. And of course in one sense this latest publishing coup does appear to confirm Gilmore's original insight. But at the same time it grossly underestimates the amount of determination and technical ingenuity needed to make sure that the aphorism continues to hold good." Hey, how much determination and technical ingenuity can YOU put in a 10-word sound bite?
- 4 April 2010: Pittsburgh Post-Gazette's Ced Kurtz reports that Stewart Brand's '[Whole Earth](#)' goes digital, and mentions his role in the early history of the Well and the EFF.
- 24 March 2010: V3.co.uk reports [EFF co-founder John Gilmore wins FSF award](#), the Advancement of Free Software award. This was also reported [in Russian by CNews.RU](#)
- 7 January 2010: The Orange County Weekly reports in [Today, Medical Marijuana. Tomorrow, Legalize It!](#) that the Drug Policy Alliance's "annual budget of \$8 million comes in part from George Soros' Open Policy Institute [I think they mean Open Society Institute --gnu] and also from about 25,000 small donors and a number of very wealthy businessmen, most notably tech guru John Gilmore of Cygnus Solutions, Peter B. Lewis of Progressive Insurance, John Glen Sperling of the University of Phoenix and George Zimmer of the Men's Wearhouse." Clearly this isn't a very well fact-checked article, and they never talked to me about it. Though I was a DPA donor in earlier years, I had stopped giving them money after 2007, because of my privacy concerns with how DPA tracks their members and donors online.
- July 10, 2009: Huffington Post's Ryan Grim: [Read the Never-Before-Published Letter From LSD-Inventor Albert Hofmann to Apple CEO Steve Jobs](#), in which I'm quoted on the connection between psychedelics and technical or scientific or business creativity.
- 9 November 2007: SuperEVA.IT: [EA regala Sim City per il progetto "One Laptop per Child"](#), about my involvement in releasing the original SimCity game (as "Micropolis") as free software for children.
- September 22, 2007: Washington Post's Ellen Nakashima on the front page: [Collecting of Details on Travelers Documented: U.S. Effort More Extensive Than Previously Known](#). My [Identity Project](#) got

http://www.toad.com/gnu/ JUL **AUG** SEP
 630 captures 14 2016 2017 2019
 1 Mar 2000 - 25 Jan 2021 About this capture

- September 2004: AP's David Kravets: [Feds Won't Acknowledge 'No Fly' List Exists](#). TSA was trying to drag my case into a secret court despite being rebuffed by sane judges.
- September 2004: Oakland Tribune's Sean Holstege: [Judges: Security fight must be in open](#). The Transportation Security Administration (TSA) tries to convene a secret court for a secret trial of my lawsuit about their secret regulations that prevent ordinary non-secret citizens from traveling unless they bring their Nazi paperwork (I mean their government-issued photo ID). The judges decide to have an ordinary trial, open to the public.
- January '03: News.com: [Hail to the...spammer-in-chief?](#) I receive spam from Joe Lieberman, a presidential candidate. Declan McCullagh reports.
- January 18, 2003: San Jose Mercury's Aaron Davis writes [Privacy activist argues against air-travel ID rule](#), covering the same hearing as below.
- January 18, 2003: Wired News's Julia Scheeres covers my lawsuit seeking to overturn unconstitutional demands that travelers provide government-issued ID, in [Judge to Hear Air ID Challenge](#)
- August '02: SF Bay Guardian picks me as a [Local Hero](#), and picks EFF as the [Best Way to Safeguard Your Freedom Online](#).
- January '02: L.A. Times: [Freedom Fighters of the Digital World](#), talking about EFF's efforts to protect civil liberties despite anti-terrorism crap shoved down americans' sheeplike throats by government thugs -- and about how I was the only one to ask about those hundreds of people imprisoned without trials, charges, or bail: "Are all the civil rights organizations afraid to step up to defend potential terrorists?"
- October '00: Scientific American, p. 36, in the sidebar "How Publius Thwarts Censors", saying that the net routes around censorship.
- June '00: USA Today: [Identity swapping makes privacy relative](#), about consumers lying to web sites, and trading supermarket identity cards, to foil snoopy companies.
- June '00: USA Today reporter Elizabeth Weise's [Tech Report](#) talks about the 6th Circuit Court of Appeals decision that affirms First Amendment protection for software source code.
- Jan '00: USA Today's Mike Snider says [Free speech at issue in DVD piracy suits](#)
- Mar '99: USA Today: [Judge: Encryption is protected speech](#) about EFF's win in the Bernstein case, declaring that "Government restrictions on exporting computer encryption programs violate free speech rights."
- Jan '99: USA Today: [Encryption code cracked in three days](#) about the DES Cracker.
- Jan '99: USA Today's [A maverick cracks the code](#) about the DES Cracker, and other parts of my life. A [sidebar](#) quotes me and David Wagner about the original meaning of "hacker".
- November '96: Wired's [Electric Word](#) section (pg. 43) covers my S/WAN project.
- August '96: My [Brain Tennis](#) match on the right to privacy, against [Dorothy Denning](#), in [HotWired](#).
- July '96: My [letter to the editor of the Economist on domain name policy](#).
- Early '96: My [interview](#) for the [Marc Canter Show](#).
- February '96: Wired's Rogier van Bakel covers Digital Telephony: [How Good People Helped make A Bad Law](#).
- June '94: Wired's Josh Quittner covers EFF: [The Merry Pranksters Go to Washington](#). The "Spy vs. Nerd" [cover](#) story.
- May '93: Wired's Steven Levy covers the Cypherpunks: [Crypto Rebels](#). That's Tim May, Eric Hughes, and me on the [cover](#), behind masks representing privacy. One of the [sidebars](#) is about my Freedom of Information tug-of-war with NSA over some documents.

Archives

I provide Internet access at some rural events, such as [Burning Man](#).

I have some [system administration insights](#) that I've learned from administering my own and my companies' machines.

the reports for the 9/11 crashes, which say nothing but:

NTSB Identification: DCA01MA065
 Scheduled 14 CFR Part 121: Air Carrier operation of United Airlines
 Accident occurred Tuesday, September 11, 2001 in Shanksville, PA
 Aircraft: Boeing 757, registration: N591UA
 Injuries: 44 Fatal.

The terrorist attacks of September 11, 2001 are under the jurisdiction of the Federal Bureau of Investigation. The Safety Board provided requested technical assistance to the FBI, and this material generated by the NTSB is under the control of the FBI. The Safety Board does not plan to issue a report or open a public docket.

Call their Public Affairs office at +1 202 314 6100. Demand to know why they're stonewalling the public on the most important airplane crashes of the decade. They've published basic Flight Data Recorder analyses, logs of radio transmissions, and radar analyses at [their FOIA site](#), but no analysis of the crash remains, nor about why the planes hit the ground -- in particular Flight 93. You can also get about 100 hours of MP3 audio recordings of 9/11/2001 radio traffic from NORAD at the [Government Attic.Org](#) web site.

See also the [Pictures from the Iraq war that the US tried to censor](#) so that Americans could not see them.




More Deflating Idiocy About Security

[I finally see some other people pointing out the low likelihood of terrorism affecting you. Try [Sam Hughes](#) on [How to fight terrorism](#).]

Your chance of having bad things happen to you *as a result of "security" measures taken by your government* is definitely on the rise. The U.S. Government has killed at least ten times as many innocent people in anti-terrorist wars after 9/11/01 than were killed by terrorist activity on and since 9/11/01. If you are an innocent person living in Afghanistan or Iraq, you are far more likely to die from the intentional act of a US Government soldier than you are to be killed by any **other** terrorists.

Many US citizens have spent time in jail because extra "anti-terrorism" searches found illegal things (that had nothing to do with terrorism). Thousands of immigrants have been imprisoned without cause, and thousands more have been deported for trivial non-safety-related crimes like overstaying a visa. (Many thousands more have left even though they were here legally, figuring out that they did not want to live in a society like what the U.S. has become.) Our former corrupt Attorney-General decided that every prosecutor and every judge should impose maximum sentences for every detected crime. Our latest corrupt Attorney-General nominee was the architect of the US torture in Guantanamo and Abu Ghraib that violated international law and every norm of civilized conduct. These actions have nothing to do with making us safer, and everything to do with building detailed control over people. A public that's constantly herded into fearfulness is far more likely to give away the blessings of liberty that we "ordained and established" a federal government to protect for us.

The Eleventh Circuit Court of Appeals came to a similar conclusion in [Bourgeois v. Peters](#), in which it found "Given that we have been on 'yellow alert' for over two and a half years now, we cannot consider this a particularly exceptional condition that warrants curtailment of constitutional rights. We cannot simply suspend or restrict civil liberties until the War on Terror is over, because the War on Terror is unlikely ever to be truly over. September 11, 2001, already a day of immeasurable tragedy, cannot be the day liberty perished in this country. Furthermore, a system that gave the federal government the power to determine the range of constitutionally permissible searches simply by raising or lowering the nation's threat advisory system would allow the restrictions of the Fourth Amendment to be circumvented too easily. Consequently, the 'elevated' alert status does not aid [a government attack on civil rights]."

http://www.toad.com/gnu/ JUL AUG SEP 14 2016 2017 2019   

630 captures
1 Mar 2000 - 25 Jan 2021

has provided positive benefits to millions of citizens. Sentencing guidelines penalizing MDMA use are an unconstitutional regulation of the freedom of thought that underlies many cherished freedoms, and should be eliminated. The re-sentencing of MDMA is part of a misguided attempt to "lock up the truth" -- or at least to lock up the truth-tellers -- about MDMA.

[Securing Internet traffic against wiretapping](#). Given the current rampage of Federal cops, it is even more important that honest citizens and businesses protect themselves from wiretapping, by deploying good encryption both in your own systems, and for communication with anyone else. If we can secure 5% of the traffic this year, we can secure 20% next year; and 80% two years out. The whole Internet will have been secured. Want to help?

[Verio censored my email, and ultimately cut off my net access, under anti-spam pressure](#). I am not a spammer, and have never sent any spam. But Verio blocked outgoing email from my machine. I was not able to send person-to-person email to my friends, my colleagues at EFF, or anyone else. I think this is wrong. Any measure for stopping spam should have as its first goal **"Allow and assist every non-spam message to reach its recipients."** I found a new provider, [United Layer](#), who is not trying to censor me. I encourage everyone to boycott Verio's Internet service, until they fix both their "Acceptable Use Policy" and their enforcement policies.

[Al Queso seeks U.S. school technologies](#). Terroristas from impoverished lands desperately seek information about US technologies that are used to educate and control U.S. students. Concerned parents should remain cowed but pliant.

In my spare time

I practice yoga, read, listen to music, travel, program, and socialize.

Why I'm Not Answering Your Email

If you've sent me email, and I haven't responded, there are three likely causes. Either I **did** send a response, and your system bounced it due to a misconfigured anti-spam filter; or my own email sorting system has decided you aren't interesting; or I haven't gotten to your message yet.

If you're a friend and you've tried emailing twice, it's probably one of our mail handling systems. I suggest phoning me. It seems that in the last few years, large numbers of ISPs have started using "blacklists", even the ones that never did before. The blacklisters hate me, so they put me on their lists, even though I have never sent a single spam message. They don't like the way I administer my machine. (I don't like the way they administer their machines either.) It will often be hard to get your ISP to admit that they are censoring your incoming email -- but ask them why you can't get email from IP address 209.237.225.253 (new.toad.com). They will tell you that that address must be a scurrilous spammer because it's on the blacklist. But you will know better.

Don't just let them put in an exception for mail from me. Get them to take off the blacklist on your incoming mail. It is usually hard -- but worth it. Who else's emails are you missing? Some of us figured out in the 1950s that blacklists were a bad idea.

gnu@toad.com, gnu@eff.org, [my PGP key](#)
Last updated November 27, 2013.