The History (and Future) of Censorship Evasion

Amy Iris Parker
University of California, Irvine
SCaLE 23x - Pasadena, CA

About Your Presenter

PhD Student, UC Irvine

Distributed and embedded systems, computer architecture, networking, social impacts

Dutt Research Group - proactive compaction

Formerly at CSU Fullerton

Analysis of evasive VPN protocols as senior project, led to this presentation

Also QEMU’s IR pipeline (Saturday, 18:15)

Secretary, Orange County DSA

Non-profit tech stack management - voting, transparency, identification, contacts

FastRequest, OSSIGINT

Lifelong *nix user

Decade-long history of using Linux; 21x

Currently running a Proxmox homelab, task automation, NixOS systems

Prior Art

Portions of this presentation were previously given at

USENIX Sec'25

Efficacy of Full-Packet Encryption for Evasive VPNs (Poster)
August 13, 2025 - Seattle, WA

LATINCOM '25

Efficacy of Full-Packet Encryption in Mitigating Protocol Detection for Evasive VPNs
November 6, 2025 - Antigua Guatemala, Guatemala

Overview

1. Early censorship - *Comstock* and libraries
2. IP, DNS, protocol blocks; *Communications Decency Act*
3. From institutions to nation-states
4. The rise (and fall) of VPNs and onion routing
5. Evasive protocols and how to find them
6. New encryption methods, alternative media, age verification laws

1

Early Censorship

The 1873 *Comstock Act* and public libraries - a time before the Internet

Before the Internet

Most communications are in-person, through written media (such as books), by the mail, by *broadcast* (radio), or through *circuits* (telegraph, telephone).

Some countries had statutory free speech protections, others did not; but all attempted to censor *assisted communications* (those not occurring in person).

Mail Censorship - the *Comstock Act*

Earliest Opportunity for Content Censorship

Mail services were essential, ubiquitous, and either government-run or government-regulated. These are the perfect conditions for uniform censorship policies to take hold.

Comstock Act - Prohibiting "Obscenities"

Adopted in 1873 (18 U.S.C. §§ 1461, 1462), the *Comstock Act* banned the sending of any "obscene" materials through the mail. Intended to restrict pornography and dissent, the Act (still on the books!) also banned contraception, abortion medication and information, and sex toys from USPS-handled services.

Other Media Censored

1. **Books**
   U.S. v. Ulysses (1933)

2. **Telegraphy**
   Civil War News Censorship

3. **Telephony**
   Oman RD 58/2024

4. **SMS/MMS**
   FCC WT No. 08-7

5. **Movies/Television**
   Hays Code, *Jacobellis*

6. **Radio**
   18 U.S.C. § 1464,
   47 CFR § 73.3999

Library Censorship

1637

New English Canaan

The Puritan government of Quincy, MA banned the *New English Canaan* due to it critiquing Puritan customs and government structures. This was considered the first book ban within the U.S.

1950s

McCarthyism

Wisconsin Senator Joseph McCarthy began a terror campaign to demand libraries remove any “pro-communist” (including LGBTQ+) material from library shelves, referring those who refused to the House Un-American Activities Committee.

1982

Island Trees v. Pico

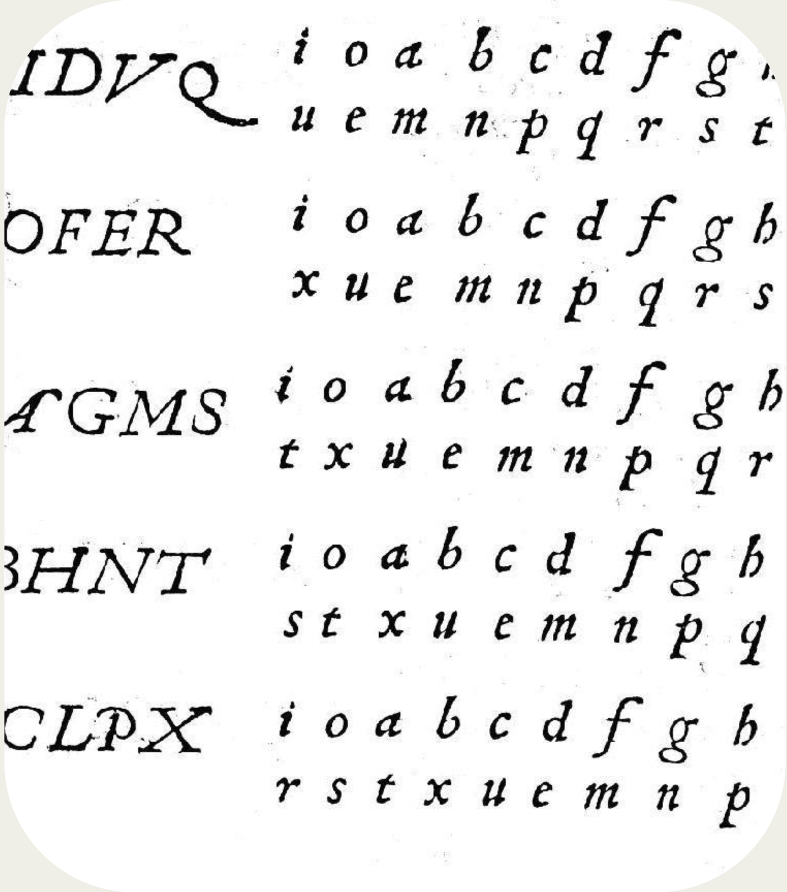
Parents and school boards attempted to ban various books from a New York school library. The ban was narrowly defeated by the Supreme Court, but book bans in school libraries are now codified in several states.

How did people evade these?

Ciphers - make the information appear random to adversaries. Works for *concealing* information, but censors often toss all ciphered messages.

Code words - blend prohibited information into allowed information undetectably. Done correctly, a censor is unable to detect that the prohibited transmission occurred at all.

Alternative media - use other methods, such as community message-passing, unmonitored radio channels, and other “underground” infrastructure.



IDVQ	i	o	a	b	c	d	f	g	
	u	e	m	n	p	q	r	s	t
OFER	i	o	a	b	c	d	f	g	h
	x	u	e	m	n	p	q	r	s
AGMS	i	o	a	b	c	d	f	g	h
	t	x	u	e	m	n	p	q	r
BHNT	i	o	a	b	c	d	f	g	h
	s	t	x	u	e	m	n	p	q
CLPX	i	o	a	b	c	d	f	g	h
	r	s	t	x	u	e	m	n	p

2

IP, DNS, Protocols

Blocking so trivial your grandmother can do it

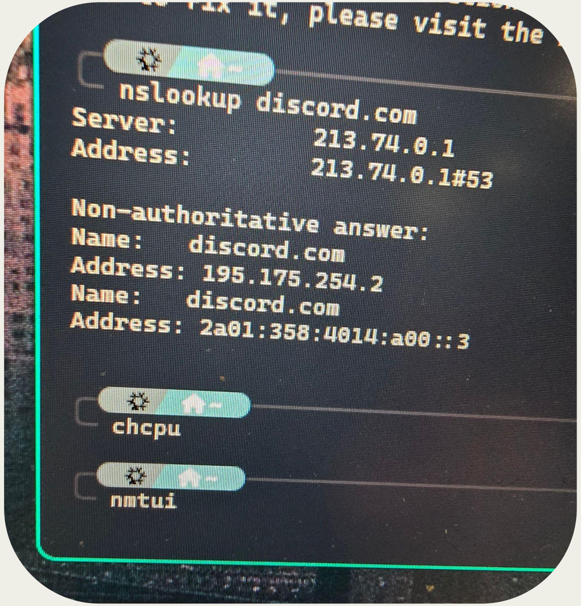
Basic IP/DNS Blocks

DNS - block domains, words

Still the most common form of censorship today - individual domain names can be blocked, as well as anything matching an expression (example: *porn*.* or *xxx*.*). Evaded through alternative DNS servers, manual route tables, new domain names, encrypted/tunneled DNS. Also exposed through TLS's SNI field.

IP - denylist addresses

More involved censors can denylist IPs manually, or add anything blocked by DNS to an IP denylist. Example: if *revolution*.* is blocked, and revolutionnow.org and forthepeople.org point to 1.2.3.4, a successful block on revolutionnow.org can also block access to forthepeople.org by adding the IP to a denylist.



```
fix it, please visit the
nslookup discord.com
Server:         213.74.0.1
Address:        213.74.0.1#53

Non-authoritative answer:
Name:   discord.com
Address: 195.175.254.2
Name:   discord.com
Address: 2a01:358:4014:a00::3

chcpu

nmtui
```

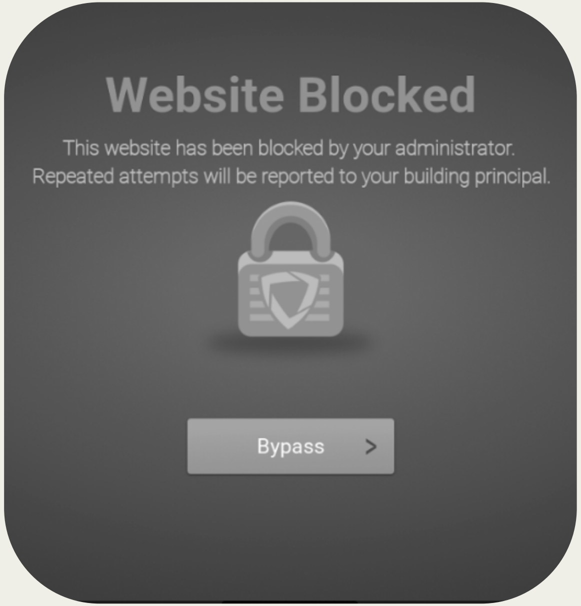
Attacks on the Web

HTTP readers, web crawlers

In unencrypted HTTP connections, a censor can read everything that is sent, often being able to block a connection after identifying prohibited phrases. Web crawlers can also preemptively identify sites with prohibited information and block them preemptively.

SNI and other metadata

TLS-secured (HTTPS) connections contain an “SNI” field, similar to HTTP’s “Host” field (another common vector). Frequently depended on due to the proliferation of load balancing and proxy services like Cloudflare, the SNI field can expose the true target/purpose of a connection. If not required for operation, leaving off the SNI can stop censors from using it as a vector.



Website Blocked

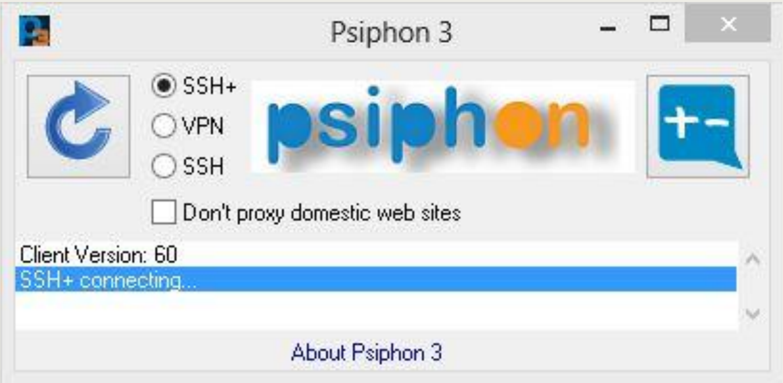
This website has been blocked by your administrator.
Repeated attempts will be reported to your building principal.

Blocking Protocols

External DNS servers are often blocked to overcome DNS evasion attempts.

Many protocols like SMTP, SSH, and IRC are blocked by strict censors due to their uncontrollability and potential for rapid information distribution.

Port-level blocks (such as 22/53), or even allowlist-only (53, 80, 443) rules, have become common to combat attempts to circumvent content restrictions by using non-content-exposing protocols.



Psiphon 3

● SSH+
○ VPN
○ SSH

□ Don't proxy domestic web sites

Client Version: 60
SSH+ connecting...

Timeline of Protocol-Based Censorship

1991

AOL's Walled Garden

America Online, one of the first consumer ISPs, initially had heavy restrictions on access to non-AOL-curated content, and would filter external content and user-submitted internal content to maintain its “family-friendly” image and approach.

1995

CompuServe & Prodigy

Prodigy blocked HTTP requests and service posts with offensive language, while CompuServe didn’t. After being sued by Stratton Oakmont, Congress passed Section 230 to permit ISPs to censor content without fear of liability.

2023

GFW, WMS 2.0

China’s *Great Firewall* deployed a new system, WMS 2.0, which focuses on packet peeking and classifying content sent over HTTP for compliance with censorship guidelines. Only 54% of Chinese websites use HTTPS, making it highly effective.

3

From institutions to nation-states

“The internet is a series of tubes” - Ted Stevens, R-AK

To Begin, South Korea!

Contrary to popular belief, China was not the first country to do widespread national internet censorship - South Korea was!

1995 Telecommunication Business Act, art. 53 - prohibits communications with “contents of harming the public safety and order or public morals”

First infrastructure for national blocks, largely through IP/DNS blocks and charges for violations upon discovery

The Golden Shield

As part of the Golden Shield Project, an all-encompassing electronic national security project by the Chinese government, the Chinese Ministry of Public Security created the **Great Firewall**, a national-level censorship regime implemented through local in-path censorship “black boxes” at ISPs.

The exact methods used by the GFW have changed over the years, but its novelty was in the uniform and total application of filtering policies across a 1.5-billion population country.

Kwangmyong

Rather than censor the Internet, North Korea took an alternative approach - *never connect to the Internet in the first place!*

Within North Korea, except for a select few with access via Ryugyong-dong (AS131279), all Internet applications run on the *Kwangmyong*, a national intranet. Although it runs on standard protocols, only internal systems - traditionally under the .kp TLD - are accessible.

Intranets remain the most effective tool for hyper-vigilant censors, but carry significant “collateral damage”.

Collateral Damage

Every system for blocking and filtering information is ultimately also going to result in some information that censors want to go through to end up getting blocked as well. This concept is called *collateral damage*.

At the nation-state level, censors need to ensure that their censorship doesn't negatively impact regular Internet operations. Even 0.6% of packets being lost is often enough for censors to back off.

4

VPNs and Onion Routing

Now offering personal FBI agents, 100% off!

The Art of Tunneling

Virtual private networks, or VPNs, are tools that do exactly as they say - they create a *virtual network*, independent of our physical networks, that is *private*. While they can be used for isolated interconnection, VPNs can also be connected to a physical network – meaning when you access that *virtual* network, you are actually accessing a physical network that *you are not physically connected to!*

Most VPNs work by capturing outgoing network traffic and sending it through a *tunnel* — nowadays, an encrypted one — to a destination server, which routes that traffic either to other clients on the VPN (if enabled) or out onto the destination server's WAN. From the user perspective, this acts as if the VPN server was sending their traffic on their behalf; the IP address presented to connected servers is that of the VPN server, not the user's.

Because the actual payloads are never directly sent over the user's network — and thus cannot be seen by censors/filters — users using VPNs to evade censorship essentially have a tunnel *through* the censorship layer. Because VPN protocols are already used innocuously, such as for connecting to an office network, the level of *collateral damage* has traditionally been too high to block VPNs directly.

Onion Routing

TOR, I2P, and other similar anonymization services use *onion routing*, which expands VPNs by adding multiple layers of routing in between the user and the final server (“exit node”).

In an onion routing setup, only the exit node can ever see what the traffic even is, and they don’t know who it came from; no node, except for the user, should be able to determine who specific content came from. However, onion routing protocols may be vulnerable to Sybil attacks if a nation-state can gain control of a critical mass of nodes.

The Fall of VPNs

2011

China Telecom/Unicom

Chinese ISPs were first ordered to engage in trivial protocol-level blocks of well-known VPN protocols. Header information and existing classification tools made common VPNs trivial to block.

2017

Widespread Adoption

As the trivial nature of VPN blocking became known and businesses relied less on VPNs for regular operations, more countries and even local institutions started blocking VPNs. 2013-2017 saw rapid growth in VPN blocks.

2020

Iran’s Allowlist

While smaller institutions had deployed allowlists before, Iran’s protocol allowlist system, first introduced in 2020, marked the first time a nation-state had imposed a national restriction on all protocols except for DNS, HTTP, and HTTPS.

5

Evasive Protocols

and ~~where~~ how to find them!

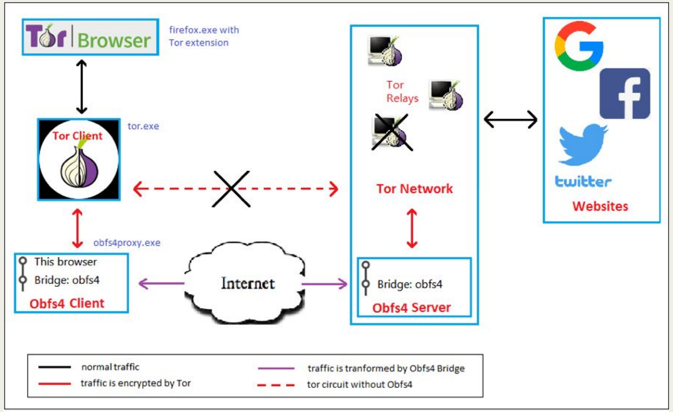
Evasive Protocols - 2 Forms

Obfuscation (Full Packet Encryption)

By far the more popular form, full-packet encryption protocols encrypt the entirety of packet, *including header/protocol information*. Unlike traditional VPNs, normal protocol fingerprinting cannot be done on FPE protocols. Data sent over an FPE protocol is indistinguishable from random noise on the network; attempts to block FPE have traditionally come with high collateral damage.

Masquerade Protocols

Used by X-VPN, several Tor plugins, and Psiphon, among others, masquerade protocols pretend to be another protocol — often HTTPS, as it is both encrypted and ubiquitous — thus acting like “code words”. No all-encompassing attacks against masquerade protocols currently exist.



Threats to Evasive Protocols

1. SNI Leaking
2. Protocol Handshakes
3. TLS 3WHS
4. Popcount/Byte-Sequences
5. Active Probing
6. Timing Attacks

FPE is Compromised

Last year, research found that even basic (C4.5) machine learning classifiers could with extremely high accuracy and essentially zero collateral damage classify between regular network traffic and FPE protocols.

We are about 3 years away from performance viability of these models. They currently have too much overhead for processing all traffic of a nation-state, but careful optimizations and use of ASICs/TPUs could make FPE models soon entirely nonviable under nation-state censors.

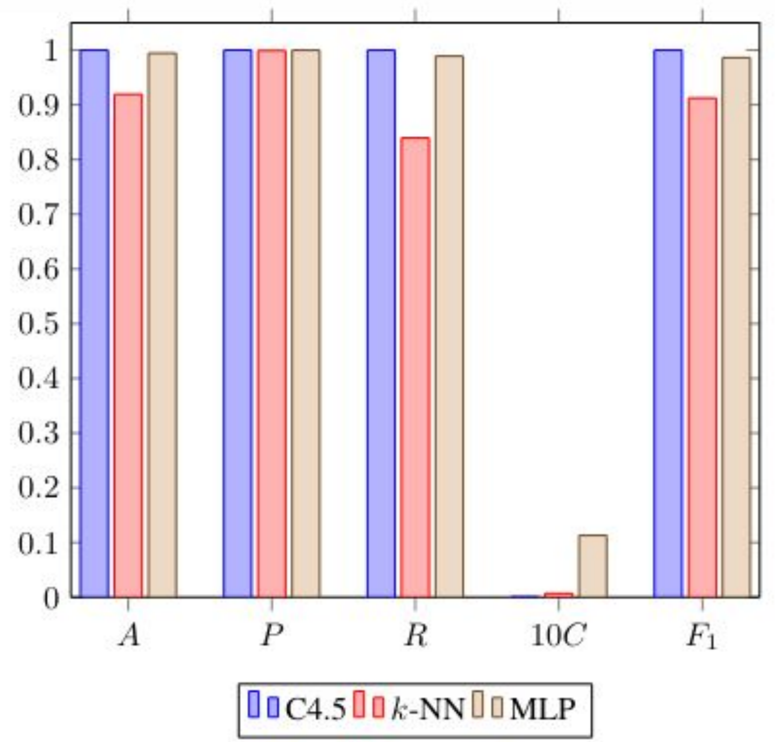


Fig. 3. Metrics from ACC vs Network testing

6

The Future of Censorship Evasion

Where do we go from here?

Masquerade Protocols

Masquerade protocols remain viable, and well-refined, robust protocols likely offer a temporary stopgap amidst escalating world tensions and increased modern censorship.

Dynamic masquerading, seen recently at USENIX by Wallis et al., could also offer a solution; if protocols themselves change faster than censors can keep up, constantly generating new protocols that users automatically switch to, then users would have continuing access. *Censorship evasion is a never-ending race between censors and users*.

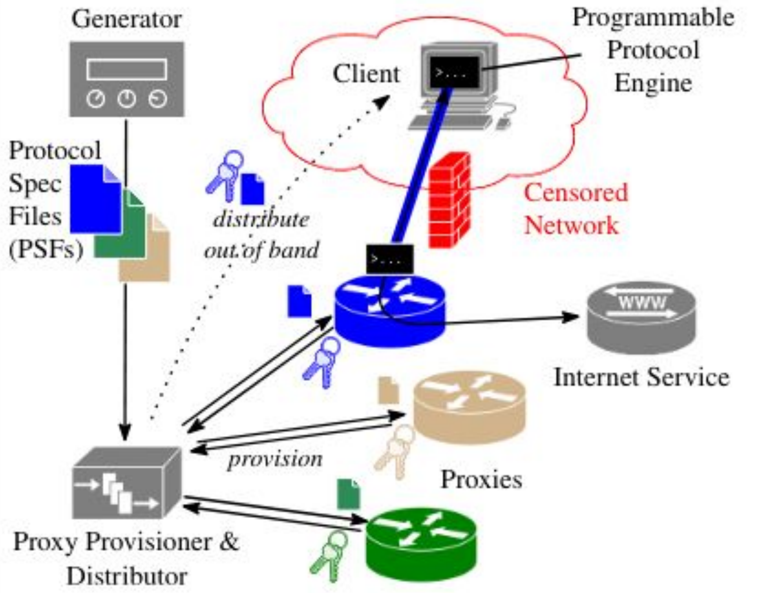


Figure 1: Schematic diagram of the UPGen censorship resistance system.

Community Networks

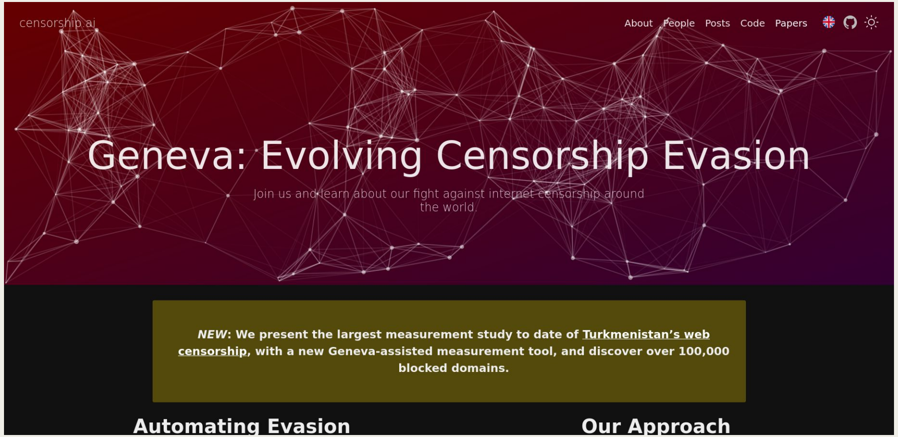
A longstanding way to defeat censorship has been **sneakernets**, which are still viable! Moving information around physically, while risky and logistically difficult, is an effective side-channel to get information flowing outside of censored networks.

Modern mesh networks, such as Meshtastic, provide a far more robust alternative system. While they can be vulnerable to malicious actors and signal jamming, Meshtastic and similar alternatives provide a basis for future community-driven information distribution.

Server-Side Evasion

Almost all censorship evasion has been client-side, as non-primary-market users access services from those not familiar with their operating conditions. More collaborative or even server-first approaches, however, have been shown viable in projects such as Geneva (which has been able to circumvent censors using entirely server-side strategies).

If developers can get serious about protecting the free and open Internet, a lot more will be possible.



Geneva: Evolving Censorship Evasion

Join us and learn about our fight against internet censorship around the world.

NEW: **We present the largest measurement study to date of Turkmenistan's web censorship, with a new Geneva-assisted measurement tool, and discover over 100,000 blocked domains.**

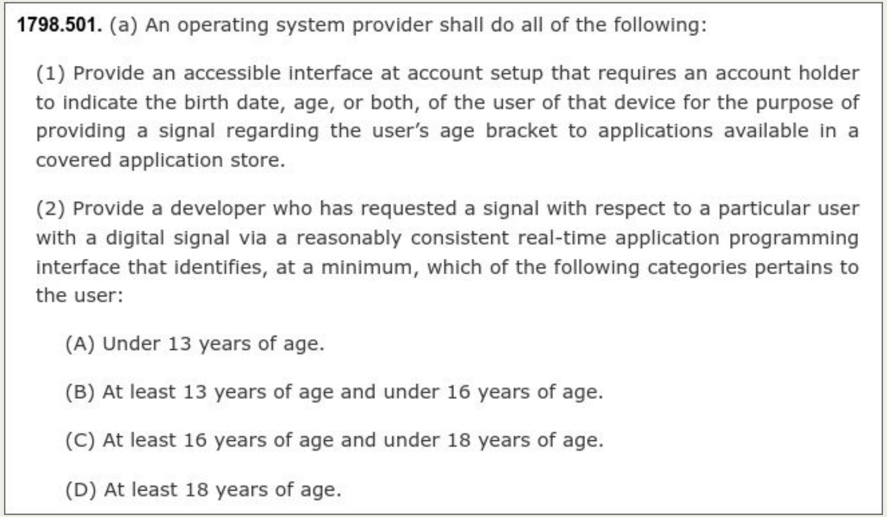
Automating Evasion

Our Approach

Age Verification Laws

Age verification laws, which generally require massive invasions into user privacy, pose a new threat of censorship, particularly targeted at those who do not want to or cannot show identification. These laws have been adopted across jurisdictions, from China and the UK to right here in California.

Future censorship evasion strategies will need to keep in mind that “mainline” technologies are at a severe risk of becoming directly tied in to censors and surveillance.



1798.501. (a) An operating system provider shall do all of the following:

(1) Provide an accessible interface at account setup that requires an account holder to indicate the birth date, age, or both, of the user of that device for the purpose of providing a signal regarding the user’s age bracket to applications available in a covered application store.

(2) Provide a developer who has requested a signal with respect to a particular user with a digital signal via a reasonably consistent real-time application programming interface that identifies, at a minimum, which of the following categories pertains to the user:

(A) Under 13 years of age.

(B) At least 13 years of age and under 16 years of age.

(C) At least 16 years of age and under 18 years of age.

(D) At least 18 years of age.

Constant Contact

As developers and engineers work on new evasion techniques, one principle must remain clear: we must remain in **constant contact** with those who actually need to use evasion systems.

Any lapse in connectivity between developers and users means that it is significantly more difficult — and more dangerous — to get programs and tools out to those who need them. Engineering against known problems must be done **now** or millions of people risk being forever cut off from the world.

References

Comstock Act of 1873, Pub. L. 42-258, cod. 18 U.S.C. §§ 1461, 1462.

United States v. One Book Called Ulysses, 5 F.Supp. 182 (S.D.N.Y, 1933)

R.B. Kielbowicz. (1994). *The Telegraph, Censorship, and Politics at the Outset of the Civil War*. Civil War History 40(2), pp. 95-118, doi: 10.1353/cwh.1994.0074

J.E. Steele. (2020). *A History of Censorship in the United States*. Journal of Intellectual Freedom and Privacy 5(1), pp. 6-19, doi: 10.5860/jifp.v5i1.7208

The Censorship of the Telegraph. (1861, May 4). Jersey City American Standard, Jersey City, NJ, USA. In *16 Months to Sumter*, www.historians.org/sixteen-months/the-censorship-of-the-telegraph/

ECDHR. (2024). *Oman's New Media Law: A Threat to Press Freedom and Free Expression*. www.ecdhr.org/omans-new-media-law-a-threat-to-press-freedom-and-free-expression/

MPAA. (1930). *Motion Picture Production Code*. historymatters.gmu.edu/d/5099/

Jacobellis v. Ohio, 378 U.S. 184 (1964), Stewart, J., concurring.

Island Trees School District v. Pico, 457 U.S. 853 (1982)

A. Brady. (2016). *The History (and Present) of Banning Books in America*. Literary Hub. lithub.com/the-history-and-present-of-banning-books-in-america/

Stratton Oakmont v. Prodigy, 23 Media L. Rep. 1794 (N.Y. Sup. Ct., 1995)

Cubby v. CompuServe, 776 F.Supp. 135 (S.D.N.Y., 1991)

Amnesty International. (2025). *Shadows of Control*. Presented at IETF Montreal 2025. Slides available at datatracker.ietf.org/meeting/124/materials/slides-124-hrpc-great-firewall-00

A. Hossain, K. Nelson, and T. Slide. (2018). *Where is the web still insecure? Regional scans for HTTPs certificates.* In *Proceedings of the 11th Norwegian Information Security Conference*, Longyearbyen, Norway, pp. 1-5.

M. Wu, J. Sippe, D. Sivakumar, J. Burg, P. Anderson, X. Wang, K. Bock, A. Houmansadr, D. Levin, E. Wustrow. (2023). *How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic*. In *Proceedings of the 32nd USENIX Security Symposium*, Anaheim, CA, USA. www.usenix.org/conference/usenixsecurity23/presentation/wu-mingshi

P. Winter, R. Ensafi, K. Loesing, N. Feamster. (2016). *Identifying and Characterizing Sybils in the Tor Network*. In *Proceedings of the 25th USENIX Security Symposium*, Austin, TX, USA. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/winter

C. Arthur. (2011). *China cracks down on VPN use.* The Guardian. www.theguardian.com/technology/2011/may/13/china-cracks-down-on-vpn-use

K. Bock, Y. Fax, K. Reese, J. Singh, and D. Levin. (2020). *Detecting and Evading Censorship-in-Depth: A Case Study of Iran's Protocol Whitelister.* In *Proceedings of the 10th USENIX Workshop on Free and Open Communications on the Internet*, online. www.usenix.org/conference/foci20/presentation/bock

A.I. Parker. (2025). *Efficacy of Full-Packet Encryption in Mitigating Protocol Detection for Evasive VPNs*. In *2025 IEEE Latin-American Conference on Communications*, Antigua Guatemala, Guatemala, pp. 1-6, doi: 10.1109/LATINCOM67778.2025.11345386

A.I. Parker. (2025). *Mitigating Protocol Detection and Traffic Analysis with Full Packet Encryption*. Senior thesis, California State University, Fullerton, pp. 1-42. Available at drive.google.com/file/d/1ml0lsMiTws_0X6oq4jSgOs_jixUH5D6o/view

Thank you!

Are there any questions?

You can also contact me via:
Phone/Signal: +1 (562) 299-8551
Matrix: @amyip.dev:matrix.org
SoCal Mesh: 62ap
Email: amy@amyip.net (keys.openpgp.org)