GPG Protecting The First Amendment

The application of encryption technology to protect citizens' constitutional rights *

Department Computer Science
Central Connecticut State University
Professor Vijayakanthan
Undergraduate Student, K

March 22, 2025

Abstract

Tasked with exploring ethical and legal aspects of a timely and relevant subtopic of information security, and in this case GNU Privacy Guard (GPG)[1], we surveyed existing literature and assembled a cogent and logical database of facts that connect this technology to legal, ethical, and psychosocial aspects of its application. The focus of this paper in particular is the freedom to articulate opinions in digital format. We explored the relevance and utility of the application of GPG and cryptographic technology to the preservation of constitutional rights and finally suggested ways to pragmatically employ this technology for the benefit of society.

Introduction

The very First Amendment to the US constitution protects Free Speech, to be more exact, it prohibits the US government from abridging the freedom of speech or the freedom of the press[2]. Indeed, it is the duty of the US government to protect the right of individuals and groups of individuals to express their ideas, thoughts, and opinions and to protect their right to freedom of assembly - much less to censor or retaliate against them for exerting these rights. The freedom to articulate and communicate one's thoughts and opinions, regardless of the medium used for this purpose, is even expressly included as a *basic human right* in the Universal Declaration of Human Rights [3] and in the international human rights law. Furthermore, apart from protections guaranteed by the US constitution, US case law provides ample evidence and support for this protection. Once such precedence enshrined in the US case law, as in Whitney versus California[4], Justia U.S. Supreme Court Center, 274 U.S. 357, in 1927:

" ... to expose through discussion falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence. – Justice Brandeis "

In other words, the remedy for harmful speech is more speech, not enforced silence.

Voltaire once said: *"I disapprove of what you say, but I will defend to death your right to say it,"* George Orwell describes freedom in the following fashion: *"If liberty means anything at all, it means the right to tell people what they do not want to hear,"* and Martin Luther King Jr. formulated the importance of the right to protest tyrannical governments as *"Somewhere I read of the freedom of speech. Somewhere I read of the freedom of the press. Somewhere I read that the greatness of America is the right to protest for right."* And, when it comes to tyrannical governments using the excuse of "national security" to squash dissent, freedom of speech, and other freedoms, Ben Franklin poignantly asserted: *"Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."*

During the Nuremberg trials, Herman Goering revealed: *"Of course the people don't want*

*Special thanks to CS undergraduate student Jaine Tiu for her invaluable contributions to the preparation of this paper.

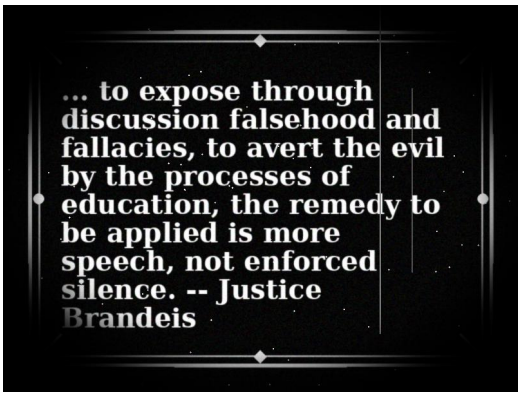

Figure 1: *Whitney versus California, Justia U.S. Supreme Court, 274 U.S. 357, 1927*

war. But after all, it's the leaders of the country who determine the policy, and it's always a simple matter to drag the people along whether it's a democracy, a fascist dictatorship, or a parliament, or a communist dictatorship. Voice or no voice, the people can always be brought to the bidding of the leaders. That is easy. All you have to do is tell them they are being attacked, and denounce the pacifists for lack of patriotism, and exposing the country to greater danger."[5]

It is in this context, that we will explore the utility of GPG as a tool to protect freedom of speech enshrined in the First Amendment and will describe technical details of GPG integration.

History of Development

We will now briefly delineate how and why GNU Privacy Guard was developed, and recite the historical context for GPG's birth and its roots in PGP.

In 1991, Phil Zimmerman created PGP, that aimed at authentication of the parties during an internet transaction. Users would utilize PGP to encrypt and cryptographically sign their messages. Its closed source nature was however diametrically opposed to transparency, which is a sine-qua-non of public trust. In 1999 Werner Koch[6] developed and released GPG version 1.0.0, which lead to the creation of the OpenPGP standard[7], that would allow interoperability of GPG with similar standards-compliant cryptographic software.

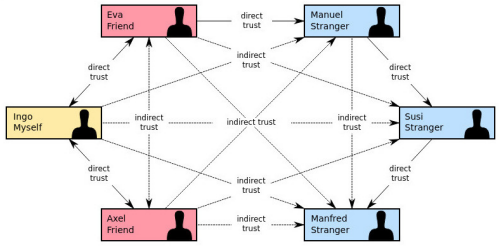

Figure 2: *Web of Trust, Source: Wikipedia*

Technical Details

GPG implements the OpenPGP standard, which is compliant with RFC 4880[8], and defines a particular format for encrypted and signed data. The aim of the OpenPGP standard is ensure interoperability as mentioned above.

Key Generation

Using public-key cryptographic algorithms, GPG generates a pair of keys: a public key, that is used by other to encrypt messages to the user, and a private key with dual function; first to decrypt above-mentioned inbound encrypted messages, and second to encrypt outbound messages to others. Others then can use the public key to authenticate the identity of the user[1].

Web of Trust

While the private key is kept secret, the public key is shared with family and friends and acquaintances, and is used by them to encrypt inbound messages by the user. The core idea and the philosophy of the GPG key management lies in what is know as the ***Web of Trust***[9]. Instead of relying on a central authority, like a Public Key Infrastructure (PKI), the Web of

Figure 3: *GPG: copyleft under GNU GPL (GNU General Public License)*

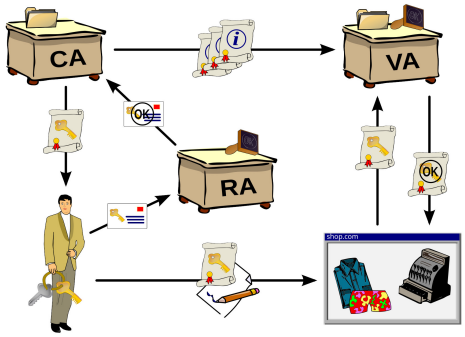

Figure 4: *Public Key Infrastructure: Wikipedia*

Trust depends on individuals couching for each other's identities. The user essentially trusts the public key of the people they know, and those friends that trust the user can extend their trust to those keys as well. In other words, indirect trust will complement direct trust.

Key Signing

What does the process of Alice publicly acknowledging that *"Alice trusts Bob"* involve? By publicly signing Bob's public key, Alice confirms that she believes that the public key authentically belongs to Bob. Now Zoe trusts Alice and signs Alice's public key, and the same time she gains some confidence in the authenticity of Bob's public key. With time, the more Zoe's friends and others sign Bob's public key, the greater will be the public's trust in the authenticity of Bob's key. In this fashion, continued key-signings progressively creates a web of interconnected trust relationships.[9]

Key Exchange

Trust does not have to be exclusively over friends. In fact, many users meet in-person and then exchange public keys and digitally sign each other's public keys. There are at times social gatherings and parties with the main theme of acquiring new friends and exchanging public keys with them. The structure of such a Web of Trust is therefore decentralized and community-driven.[10]

Public Key Infrastructure

The public key infrastructure wholly relies on Certificate Authorities (CAs). CAs are "trusted" entities that issue and manage digital certificates, and verify the identity of certificate applicants.[11] Although many intermediate CAs exist, they all rely on the *root certificates* issued by *root certificate authorities,* in other words the top-level CAs, which are supposed to be the foundation of trust in the PKI hierarchy. This system at its core relies on *chain of trust* and *delegation of authority.*

Although the exact numbers fluctuate, there are only a little over a dozen main commercial certificate authorities, including: DigiCert, Sctigo, GoDaddy, GlobalSign, etc; but numerous governmental certificate authorities, including: U.S. Treasury Root Certification Authority (TRCA), U.S. Treasury Operational Certification Authority (TOCA), NASA Operational Certification Authority (NOCA), Social Security Administration Certification of Authority (SSACA), Department of Homeland Security Certification Authority (DHSCA), etc.[12]

Trusting Central Authority

It all boils down to trust. And trust can only be based on history and track record. In this paper, we will include historical cases in and outside the US. This history intricately elucidates the practical, legal, and ethical issues surrounding reliance on a few "trusted" root authorities.

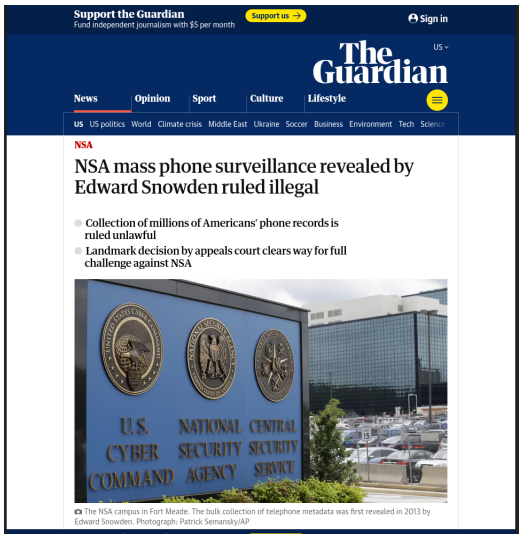

Figure 5: *NSA mass surveillance ruled illegal: Guardian 2015*

We will begin with evaluating the track record of commercial certificate authorities and after that the track record of governmental certificates of authority. Here are a few examples of the failure of the centralized trust systems involving commercial entities:[13]

DigiNotar 2011

This Dutch CA was compromised and fake certificates were issued and used for "man-in-the-middle" attack against Iranian Gmail users. The result was DigiNotar's bankruptcy and a significant loss of trust in this centralized system of certification.[19]

Symantec 2015, 2015, 2017

Symantec gained notoriety for not once but even while on probation issued over 100 bogus certificates, leading to Symantec ultimately being distrusted by all major platforms due to malfeasance. Symantec sold its business and was re-branded as DigiCert, which is still one of the main issuers of certificates.[20]

WoSign 2015, 2016, 2017

WoSign and its subsidiary were caught backdating certificates and engaging in other improper practices.[13]

The list of the ways and incidents, where commercial entities have historically failed and betrayed the public trust is long [13] [14]. On the other hand, outside the realm of commercial entities, incidents and scandals involving US government agencies and abuse of power in connection to their claimed authority to issue certificates is also eye-opening. Such incidents involving the misuse of their certification authority includes the following:

NSA 2013

Widespread illegal surveillance of not only foreign nationals but US citizen by the NSA, that was brought to light by Snowden documents in 2013, including man-in-the-middle attacks, fake websites, that received traffic re-directed from NY ATT-server closets, interception of protected information, and injection of poisoned data. The Snowden documents also revealed NSA's ability to decrypt current *commonplace* encryption protocols, that they had previously falsely claimed to be secure.[15]

Crypto AG, Operation Rubicon

For decades the CIA and the German BND secretly owned and controlled the Swiss Company Crypto AG and distributed devices rigged with backdoors for the purpose of eavesdropping worldwide[16].

Clipper Chip 1990

The NSA developed a backdoored *Clipper Chip* with a compromised escrow key, that would allow illegal surveillance by the government[17].

Dual Elliptic Curve Deterministic Random Bit

This was a backdoored cryptographically insecure random number generator promoted

Figure 6: *Clipper Chip: Crypto Museum [17]*

by the NSA, and this illegal activity only came to light with Edward Snowden's 2013 revelations[18].

Legal and Ethical Perspectives

The main philosophical, socio-political, legal, and ethical questions arising from these complex, multilayered context are as follows:

Does this illegal surveillance constitute beneficence or malfeasance. What cross-relationships exist among these various issues? Should a US citizen be happy, if a powerful government, a metaphorical all-knowing parent, uses its might and all its tools, including legal and illegal devices and strategies, to stay in power, to protect the status quo and the current state of an uneven distribution wealth among US citizens, and makes decisions for its naive children, and continues to pursue *full spectrum dominance* and to further the flourishing of *American Exceptionalism*? Should a US citizen be happy, if a real-life Jack Nickelson poignantly and loudly exclaims "You want The Truth? You can't handle The Truth!" OR, should a US citizen demand real participation in the decision-making process, so that she or he can represent and protect their specific interests; as opposed to the make-belief of soft-money-accepting elected officials voting against the interests of the average citizen and in favor of the billionaires at every turn? Should a US citizen demand transparency and accountability? Should a US citizen insist on the *division of powers* and be mortified to see all three branches rolled into one and in the clutches of a small, powerful, mostly unelected elite. Should a US citizen worry about the unfree future awaiting his or her children in this neo-feudalistic social system?

Multilayered Ethical Concepts and Perspectives

After applying these contrasting ethical and legal concepts one can finally recognize the nuanced cross-relations among these diametrically opposed view-points and philosophies, each one having very different implications which we must consider.

It is only after gaining a more comprehensive world-view, that a US citizen would truly be able to give an informed answer to the question: Is it okay, if Big Brother[25] reads my emails, listens to my phone calls, collects every bit of information available about my profile, either directly or through Palantir in a roundabout fashion to circumvent existing laws that protect civil liberties? Should I or my children, one day develop the courage to become politically active and participate in some pro-peace movement, would Big Brother descend upon my life (or their lives) and destroy it all in a flash?

It is my position, being fully aware of all objections on the other side, that freedom trumps servitude, and I am confident, that I can reasonably defent my position against all those who woould objection, specifically those who dishonestly use the cudgel "but what about national security." It is partly in this context, and while considering various aspects of this complex issue, that the questions regarding cryptography, secure communications, Web of Trust versus centralized certificate authorities should be pondered upon. But first let us look at the concept of "the government."

What are the constituent *parts* of the government? If we dissect this entity, we will recognize, that it consists of *individual human beings*, the atomic units of its composition. The government constitutes a complex system and,

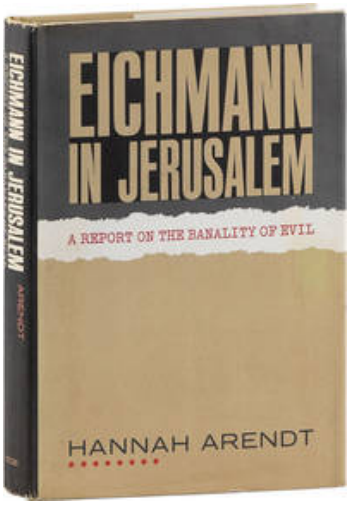

Figure 7: *Hannah Arendt: The Banality of Evil*

like all complex systems exhibits, *emergent behavior*. This emergent behavior is however a direct function of the mode of operation of its atomic subunits, namely the individuals. So first, we have to understand how the subunits of this bureaucracy function. I believe, that Hannah Arendt's insight can greatly assist us in exploring the psyche of each one of these atomic subunits, the modus operandi of each bureaucrat. Only then can we shed light on the multi-layered relationship of this superorganism. But, who was Hannah Arendt?

Hannah Arendt

Hannah Arendt was a political theorist, who in 1961 covered the trial of Adolf Eichman, a key Nazi SS officer organizing the mass murder of communists and socialists and Jews. In her book, The Banality of Evil, she describes, that she expected to see a monstrous, hate-filled figure. Instead what she found, was a pedantic bureaucrat, who was not driven by ideological fever or sociopathic malice, but by the desire to fit in, obey orders, and be efficient. She saw a cog in the machine that was incapable of independent judgment and lacked the capacity to see the long-term consequences of his actions. In other words, although his actions were heinous, his motivations were petty and

Figure 8: *Vietnam War Veterans, "Peace is Dignity" 1966*

ordinary. Eichman's story showcased how ordinary people can commit extraordinary atrocities. The 2023 movie *The Zone of Interest* also builds on the main theme of The Banality Evil.

So how can the ordinary man not become a cog in a machinery that aims to destroy freedoms, including the freedom of speech, and violate the civil rights of ordinary citizens just like this very ordinary man, who only to aims to fit in, to obey, to be a team-player, and to be an obedient citizen?

The Courage to Think and to Speak

The answer to the above question is this: He must think. He must think freely. He has the moral duty to free his thought. He has the ethical duty to read and to educate himself. Towards his own progeny, he has the ethical duty to be brave. Brave to read, brave to learn, and brave to think. A good citizen is morally obligated to grow. The next question is what environment is particularly conducive to growth, and what role does open and free social discourse play in this process of maturation? What forces oppose free social discourse?

Opposing Free Social Discourse

What is the historical precedence, when it comes to suppression of free speech? Are there any examples?

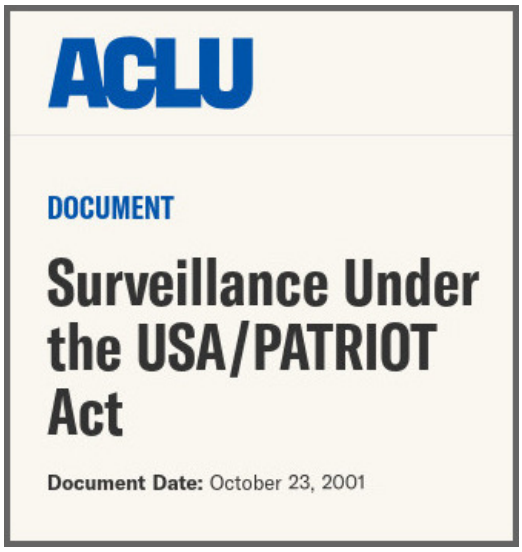

Figure 9: *ACLU Document: 2001[22]*

Vietnam War Era

During the Vietnam War the government engaged in extensive surveillance of anti-war activists and civil rights leaders. The FBI routinely disrupted and attempted to discredit dissent group using legal and illegal means (COINTELPRO)[21]. These activities included wiretapping, infiltration, and spread of disinformation. These attacks on free speech had a very significant chilling effect and successfully suppressed US citizens' constitutional rights, including freedom of speech and freedom of assembly[21].

Patriot Act

The Patriot Act has undoubtedly been the single most intrusive action ever undertaken by the US government against US citizens. Its chilling effect on free speech does not need to be belabored. National Security Letters are used to subpoena records without any judicial oversight and the accompanying gag order prevents the recipients from notifying the citizens, peace activists and the like, that they have been targeted. The intrusion and pace of violation of constitutional rights of the citizens has significantly be increased by the introduction of *fusion centers*[23], where agencies share data. No meaningul protection for citizens' right to privacy exists. The chilling effects of such pervasive and invasive surveillance is undeniable[22].

Conclusion: GPG Facilitates Social Discourse

So how can GNU Privacy Guard technology facilitate freedom of speech and encourage social discourse? Just as invasive and pervasive surveillance has a chilling effect on communication among friends and family, protection against such unconstitutional intrusion would encourage friends and people who think alike to express themselves more freely and exchange ideas, without the fear of suddenly being targeted, and seeing their life and livelihood evaporate in a flash in front of their eyes. Typically, however, citizens only engage in deep philosophical and political discourse with their close family members and friends and not necessary when exchanging business email or assisting their accountant to complete tax forms. Hence GPG only needs to be used for a limited number of communications between close friends; communication that would otherwise not blossom and wither, when exposed to the destructive effect of surveillance. In this digital age, widespread surveillance has created a modern-day panopticon. People internalize the feeling of being watched. This leads to self-censorship and a reluctance to engage in dissenting or unconventional thought. However, once citizens truly believe that they have exited the panopticon, many will likely feel motivated to discuss social and budgetary matters; issues that deeply affect their everyday lives. Open debate on these matters is vital for democratic societies. Informed citizens who freely express their opinions are better equipped to advocate for change and social progress[24].

The Future: The Hybrid Method

In the future likely hybrid methods will flourish. Since the number of GPG keys that need

to be exchanged and stored grows with $O(n^2)$, realistically GPG and the decentralized method of Web of Trust should be the primary method of encrypting communication among friends and family members, the inner circle, since that conversation would likely include political discourse. The fall-back method would still remain the centralized Root Certificate Authority validation of the identity of individuals and entities. It is my now my position, that in this fashion an adequate breathing space can be created for US citizens, who could then start engaging in free social and political discourse, without fearing Big Brother's[25] devastating retaliation[26].

" Posterity will be the beneficiary. – me" □

Acknowledgments

My heartfelt thanks go to Dr. Joseph Paige, Ombudsperson at Central Connecticut State University, for his warm encouragement and insightful advice, which have been a great comfort and assistance during my final semester. I would also like to thank Professor Chad Williams for his invaluable support and guidance throughout my graduate studies.

References

[1] "GNU Privacy Guard." Wikipedia, Wikimedia Foundation, As of 21 March 2025, https://en.wikipedia.org/wiki/GNU_Privacy_Guard

[2] U.S. Constitution - First Amendment | Resources | Constitution Annotated | Congress.Gov | Library of Congress, constitution.congress.gov/constitution/amendment-1/. Accessed 21 Mar. 2025.

[3] "United Nations Human Rights System - Global Freedom of Expression." Global Freedom of Expression, 2019, globalfreedomofexpression.columbia.edu/law-standards/united-nations-human-rights-system/.

[4] "Whitney v. California | the National Constitution Center." National Constitution Center – Constitutioncenter.org, 2022, constitutioncenter.org/the-constitution/supreme-court-case-library/whitney-v-california.

[5] DWOOD. "Intellectual Freedom Quotes." About ALA, 1 Aug. 2017, www.ala.org/aboutala/intellectual-freedom-quotes.

[6] Wikipedia Contributors. "Werner Koch." Wikipedia, Wikimedia Foundation, 5 Jan. 2025.

[7] "Pretty Good Privacy." Wikipedia, 5 Oct. 2022, en.wikipedia.org/wiki/Pretty_Good_Privacy#OpenPGP.

[8] Callas, J., et al. "OpenPGP Message Format." Www.rfc-Editor.org, 1 Nov. 2007, www.rfc-editor.org/rfc/rfc4880, https://doi.org/10.17487/RFC4880.

[9] Wikipedia Contributors. "Web of Trust." Wikipedia, Wikimedia Foundation, 4 June 2019, en.wikipedia.org/wiki/Web_of_trust.

[10] Wikipedia Contributors. "Key Signing Party." Wikipedia, Wikimedia Foundation, 20 July 2024.

[11] Archiveddocs. "What Are ca Certificates?: Public Key; Security Services." Learn.microsoft.com, 9 Aug. 2010, learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)?redirectedfrom=MSDN.

[12] Wikipedia Contributors. "Certificate Authority." Wikipedia, Wikimedia Foundation, 9 Jan. 2020, en.wikipedia.org/wiki/Certificate_authority.

[13] "Timeline of Certificate Authority Failures - SSLMate." Sslmate.com, sslmate.com/resources/certificate_authority_failures.

[14] Hadan, Hilda, et al. "A Holistic Analysis of Web-Based Public Key Infrastructure Failures: Comparing Experts' Perceptions and Real-World Incidents." Journal of Cybersecurity, vol. 7, no. 1, 1 Jan. 2021, https://doi.org/10.1093/cybsec/tyab025.

[15] Wikipedia Contributors. "Edward Snowden." Wikipedia, Wikimedia Foundation, 16 Mar. 2019, en.wikipedia.org/wiki/Edward_Snowden.

[16] "Rubicon." Www.cryptomuseum.com, www.cryptomuseum.com/intel/cia/rubicon.htm.

[17] "Clipper Chip." Www.cryptomuseum.com, www.cryptomuseum.com/crypto/usa/clipper.htm.

[18] "Dual_EC_DRBG." Wikipedia, 13 Mar. 2022, en.wikipedia.org/wiki/Dual_EC_DRBG.

[19] Wolff, Josephine. "How a 2011 Hack You've Never Heard of Changed the Internet's Infrastructure." Slate Magazine, 21 Dec. 2016, slate.com/technology/2016/12/how-the-2011-hack-of-diginotar-changed-the-internets-infrastructure.html.

[20] "DigiCert to Acquire Symantec's Website Security Business." Digicert.com, 6 Mar. 2024, www.digicert.com/blog/digicert-to-acquire-symantec-website-security-business. Accessed 22 Mar. 2025.

[21] FBI. "COINTELPRO." FBI, 2020, vault.fbi.gov/cointel-pro.

[22] "PATRIOT Act Fears Are Stifling Free Speech, ACLU Says in Challenge to Law | American Civil Liberties Union." American Civil Liberties Union, 20 Sept. 2005, www.aclu.org/press-releases/patriot-act-fears-are-stifling-free-speech-aclu-says-challenge-law.

[23] https://www.aclu.org/news/national-security/secret-domestic-surveillance-program-about-get-pulled-out-shadows

[24] https://politicalscience.yale.edu/publications/open-democracy-reinventing-popular-rule-twenty-first-century

[25] Wikipedia Contributors. "Nineteen Eighty-Four." Wikipedia, Wikimedia Foundation, 16 Feb. 2019, en.wikipedia.org/wiki/Nineteen_Eighty-Four.

[26] George Orwell. George Orwell's 1984. Internet Archive, archive.org/details/GeorgeOrwells1984.