THE RIGHT TO SILENCE IN THE DIGITAL AGE: RECONCEPTUALISING ADVERSE INFERENCES FROM THE REFUSAL TO DISCLOSE PASSWORDS

Prof. Shakeel Ahmad, Dean & Professor, D/O Law, AMU

Ved Prakash Singh, Research Scholar, D/O Law, AMU

ABSTRACT

The right to silence, a cornerstone of criminal justice, is being profoundly challenged in the digital era. With the increasing use of encrypted digital devices and data protection mechanisms, courts and law enforcement agencies face growing difficulties in obtaining access to evidence. This paper critically examines the tension between the right to silence and the legal consequences of refusing to disclose digital passwords. It explores how traditional interpretations of adverse inferences drawn from silence or non-cooperation—must be reevaluated in the context of modern technology. By analyzing contemporary case law, statutory frameworks, and human rights principles, the study argues that compelling password disclosure infringes upon the privilege against self-incrimination and the broader right to privacy. The paper proposes a reconceptualization of legal doctrines to balance state interests in crime prevention with individual digital rights. Ultimately, it contends that the right to silence should evolve to encompass digital silence—protecting individuals from coercive demands to reveal access credentials—thereby reaffirming the fundamental presumption of innocence in an increasingly data-driven world.

Keywords: Right to Silence, Digital Age, Password Disclosure, Adverse Inference, Self-Incrimination, Privacy Rights, Digital Evidence, Cyber Law, Criminal Justice, Human Rights.

INTRODUCTION

The Digital Turn and the Silent Person

The advent of ubiquitous computing and encrypted information storage has ushered in a profound shift in how evidence is generated, stored, and accessed. In the past, the right to silence and protections against self-incrimination were mostly relevant in interrogations, confessions, or testimony. But today, suspects may possess digital devices—smart phones, laptops, cloud accounts-locked behind passwords or encryption keys. The question thus emerges: when authorities demand disclosure of passwords or compel decryption, does that demand violate the individual's right to remain silent? This inquiry is more than a technical curiosity; it is a constitutional fault line in a data-driven world.

Scholars have noted that encrypted devices pose a hybrid challenge: they implicate both the Fourth Amendment (seizure/search) and the Fifth Amendment (self-incrimination) in U.S. law and analogous doctrines in other legal systems. (Sacharoff, 2018)[1] Courts have been deeply divided over when, and to what extent, compelling a person to surrender or unlock a device infringes on protected rights. (Veas et al., 2025)[2]

While much of the debate has taken place in U.S. constitutional law, similar tensions are emerging globally: as states enhance powers to mandate disclosure of digital credentials or impose obligations on service providers, the fundamental principle beneath the right to silence must be reexamined in the digital age.

Traditional Doctrine of Adverse Inferences and Silence

In classical criminal procedure, the right to silence is tied to a prohibition on drawing adverse inferences from a suspect's refusal to testify or answer certain questions. Put simply, a defendant should not be penalized for choosing silence.

Over time, many jurisdictions have permitted *limited* adverse inferences (e.g., inference of consciousness of guilt) if certain safeguards are satisfied. But these doctrines were developed

[1] . Sacharoff, L. (2018). Unlocking the Fifth Amendment: Passwords and encrypted devices. 87 Fordham Law Review, 203-251.
[2] . Veas, M., et al. (2025). Compelled decryption and digital rights (volume and page numbers not located).

in an era when the "silent" act was a refusal to speak—not a refusal to cooperate with digital access demands.

The extension of adverse inference reasoning into the digital realm raises novel conceptual problems: is refusing to divulge a password equivalent to remaining silent? Or is it a form of (indirect) assistance to the prosecution? Some courts treat refusal to hand over encryption keys as akin to refusing to testify — thus allowing adverse inferences—while others refuse to treat it as testimonial at all. (McGregor, 2010)[3] the line between silence and compelled "act" becomes blurred when a suspect must choose between self-incrimination and forced cooperation.

Moreover, the so-called "act of production doctrine" (derived from Fisher and its progeny in U.S. jurisprudence) maintains that compelling someone to produce documents or physical evidence is sometimes testimonial (and thus protected) if the production reveals *possession, control,* or *authentication* of those documents. (Sacharoff, 2018)[4] the doctrine has been stretched and contested when the object is a digital device or password—and the traditional lines of "speech" vs. "conduct" falter.

The Privacy and Dignity Stakes

One core value underpinning the right to silence is the protection of the inner workings of the mind: the content of one's thoughts, memories, and mental associations. A password is arguably part of that mental domain. When the state demands that a person "reveal what only resides in their mind," the individual is placed in a coercive bind: either surrender private mental material or face legal penalty for refusal. Advocates argue that compelling password disclosure undermines individual privacy, autonomy, and human dignity.

The European and comparative human rights framework likewise recognizes that procedural safeguards are needed for compelling digital disclosures to avoid disproportionate interference with the privacies of individuals. At the same time, the state has a legitimate interest in investigating crime, recovering evidence, and ensuring the efficacy of digital forensics. This tension—between state power and individual rights—becomes acute where digital evidence is

[3] **.** McGregor, N. K. (2010). The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege. (volume and page numbers not located)

[4] **.** Sacharoff, L. (2018). Unlocking the Fifth Amendment: Passwords and encrypted devices. 87 Fordham Law Review, 203-251.

central to prosecutions. The challenge is how to balance these interests without hollowing out the presumption of innocence or permitting unrestrained fishing expeditions.

Fragmentation in Case Law: Compelled Decryption in Practice

In practice, courts have adopted divergent approaches when confronted with compelled access to encrypted or password-protected data. Some courts have compelled production or decryption under statutes or court orders; others have resisted on self-incrimination grounds. (Veas et al., 2025)[5]

For example, in *United States v. Kirschner*, the court held that compelling the defendant to divulge a password to an encrypted file would violate the Fifth Amendment, as it required producing

"specific testimony" revealing control and existence. (Kirschner, 2010)[6] conversely, in *United States v. Fricosu*, the court ordered the suspect to produce an unencrypted version of a hard drive under the All Writs Act, essentially compelling decryption. (Fricosu, 2012)[7] *In re Boucher*, the district court originally quashed a subpoena for a passphrase on Fifth Amendment grounds, but the appellate court later compelled production of the unencrypted data, concluding the act fell outside protection. (In re Boucher, 2009)[8]

These conflicting decisions reflect deeper doctrinal confusion around when a compelled act is 'testimonial' and when it is merely 'conduct.' Moreover, some cases lean heavily on narrow technical reasoning (e.g., whether the government already knows of the existence of the files) rather than a principled test of inference or compulsion.

The Foregone Conclusion Doctrine and Its Limits

A central concept in this terrain is the *foregone conclusion* doctrine. Under this doctrine, if the state can show with reasonable specificity that it already knows the existence, location, and authenticity of the files or data, then compelling their production or decryption does *not* add any new testimonial content, and thus does not violate the privilege against self-incrimination.

[5] . Veas, M., et al. (2025). Compelled decryption and digital rights (volume and page numbers not located).
[6] . United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010).
[7] . United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012).
[8] . In re Boucher, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

This doctrine has been applied to justify compelled production of documents in non-digital cases (Fisher). (Sacharoff, 2018)[9]

In the digital sphere, however, the doctrine faces serious challenges. Encryption can hide not only *contents* but *existence* of certain files. It may be unclear whether the state truly *knows* what is on the device, or whether it merely speculates. Recent scholarship has proposed refinements, especially from fields of computer science, that demand the state bear the burden of proving that no new testimonial act occurs. (Cohen, Scheffler & Varia, 2022)[10] they introduce notions like "demonstrability" to test whether a compelled action is truly a foregone conclusion.

Critics caution that the doctrine, if overextended, can swallow the privilege: the state might always (or almost always) claim knowledge of filenames, locations, or metadata, thus erasing protection. The tension is especially sharp when police demand broad decryption orders, rather than limited access to identified files.

A New Framework: Reconceptualizing Adverse Inference in the Digital Context

Given the doctrinal ambiguity and technological complexity, this paper calls for a reconceptualization of how adverse inferences should operate when suspects refuse to disclose passwords or assist in decryption. Rather than simply porting over analog-era doctrine to digital contexts, we must develop a digital-sensitive framework grounded in principles: minimization, specificity, procedural safeguards, burden of proof, and proportionality.

The proposed framework recognizes three layered questions:

1. **Is the compelled act testimonial (versus non-testimonial conduct)?**

   We must scrutinize whether disclosure of the password reveals mental content (possession, control, or authenticity) or whether it is a neutral act akin to handing over a key.

[9] **.** Sacharoff, L. (2018). Unlocking the Fifth Amendment: Passwords and encrypted devices. 87 Fordham Law Review, 203-251.
[10] **.** Cohen, A., Scheffler, S., & Varia, M. (2022). Can the Government Compel Decryption? Don't Trust — Verify. (preprint / technical article; volume and page numbers not in a traditional journal)

2. **If testimonial, can the foregone conclusion doctrine apply?**

   The government should bear a strict burden to show it already knows the specific facts the act would reveal. Courts should not grant wide orders on speculation or fishing expeditions.

3. **If protection applies, what procedural regime governs adverse inferences?**

   Should refusal to decrypt lead to adverse inference at trial? If so, under what limits? What safeguards (e.g., judicial oversight, narrow scope, in camera review, evidentiary thresholds) must be in place?

Under a robust design, an adverse inference may be permissible—but only when the government satisfies stringent conditions: the existence of the files is known, the demand is narrowly tailored, the suspect has a real capacity to comply, and the inference is proportionate and subject to judicial checking.

Contribution and Roadmap

This paper makes three main contributions. First, it brings clarity to the doctrinal confusion surrounding compelled digital disclosures and reorients the debate from a purely technical battlefield to one of constitutional principle. Second, it proposes a structured, balanced test that accommodates both the state's investigatory needs and the individual's right to silence and privacy. Third, it offers comparative and normative perspectives, considering how jurisdictions beyond the U.S. might grapple with the same tension in their criminal procedure and human rights regimes. In Section II, the paper will trace the doctrinal evolution of the privilege against selfincrimination and the act of production doctrine, showing how they have been adapted (or misadapted) to digital contexts. Section III will analyze in detail the technical dimensions of encryption, passwords, and cryptographic deniability, and their implications for testimony. Section IV will examine landmark cases and divided approaches across jurisdictions, drawing lessons from successes and failures. Section V will outline the proposed reconceptualized framework for managing adverse inferences, with recommended procedural safeguards and illustrative hypotheticals. Finally, the Conclusion will reflect on the broader consequences: how a robust digital right to silence upholds the presumption of innocence in the information society.

CONCLUSION

The evolving landscape of digital technology demands a redefinition of the right to silence in the context of compelled password disclosure and encrypted data access. As courts and legislators struggle to reconcile traditional legal doctrines with modern technological realities, it becomes clear that applying analog-era concepts to digital contexts without adjustment risks eroding fundamental rights. Compelling individuals to disclose passwords or decrypt devices directly engages the privilege against self-incrimination and the right to privacy—cornerstones of a fair justice system. While the state's need to obtain evidence and combat cybercrime is undeniable, such objectives must be pursued within the limits of constitutional safeguards and proportionality. The reconceptualization of adverse inferences from silence in digital contexts should focus on maintaining the balance between effective law enforcement and individual liberty. A digitally aware framework—anchored in the principles of voluntariness, necessity, and judicial oversight— can ensure that technological advancement does not become a tool of coercion. Ultimately, the right to digital silence should be recognized as an essential extension of the right to remain silent, preserving the dignity, autonomy, and mental privacy of individuals in an age where data is both power and vulnerability.