What is Cryptography Hiding from Itself?

Diego F. Aranha[1] and Nikolas Melissaris[2]

[1]Aarhus University, Denmark, dfaranha@cs.au.dk
[2]IRIF, CNRS & Université Paris Cité, France, nikolas@irif.fr

Abstract

The European Commission's 2022 proposal for a regulation on child sexual abuse material, popularly labelled *ChatControl*, obliges online services to detect, report, and remove prohibited content, through client-side scanning. This paper examines the proposal as a case of *undone science* in computer security ethics: a domain where technical feasibility and rights-compatibility questions remain systematically underexplored. Combining legal analysis with philosophy of technology, the paper argues that client-side scanning transforms end-to-end encryption from a right to secrecy into a conditional privilege of use. By integrating Isaiah Berlin's concept of negative liberty, Langdon Winner's account of the politics of artifacts, and David Hess's notion of undone science, the analysis traces how design choices become moral constraints. The discussion situates the European debate within broader concerns about proportionality, epistemic selectivity, and the governance of digital infrastructures. Ultimately, the study shows that the controversy over ChatControl is not only about privacy or child protection but about the epistemic norms that define what counts as legitimate technological knowledge.

1 Science under pressure

Every scientific field inherits a moral horizon, a tacit sense of what it serves. For computer science that horizon was knowledge and efficiency and for cryptography specifically, it was trust. Over time, the boundary between protecting and controlling blurred. Funding priorities, regulatory expectations, and the rhetoric of *safety* began to define legitimacy. What once defended autonomy, risks becoming a service industry for institutional anxiety.

We are now asked to build systems that guarantee both privacy and preemptive policing, something that is impossible to make possible. *Client-side scanning* (CSS) embodies this demand. A technical attempt to reconcile incompatible moral goals by hiding coercion in software. The paradox is pretty old and it shows up when a society gets frightened enough to monitor everyone and calls its vigilance "freedom".

Following Hess [8], this pressure reflects a deeper epistemic condition: the emergence of *undone science*, where essential lines of inquiry remain unexplored because they would unsettle prevailing political or institutional priorities. In Jasanoff's terms, science and governance are *co-produced* [9] and each defines the other's boundaries of legitimacy. If the moral vocabulary of a discipline narrows under policy urgency, then ignorance becomes a form of compliance.

2 The ChatControl moment

In 2025, the European Union's proposed *Child Sexual Abuse Regulation (CSAR)* (known as *ChatControl*) reached a decisive stage. Under the plan, platforms would be obliged to scan users' private messages and images and report matches to authorities. Council votes are scheduled for mid-October 2025. Several governments remain undecided, while over seven hundred scientists have urged rejection, calling the plan technically infeasible and democratically dangerous [10, 5, 6, 13].

Technically, the Regulation introduces a regime of *detection orders* requiring platforms to deploy scanning tools like hash matching, perceptual matching, and upload moderation, reporting results to a newly created European Center for Child Sexual Abuse [7, 1]. Although described as technology-neutral, these mechanisms presuppose the feasibility of universal inspection before encryption, a claim that remains empirically untested and therefore exemplifies undone science in regulatory design.

Proponents describe ChatControl as a proportional child-protection measure while opponents see the first legal mandate for universal digital search. Both sides invoke "security", but mean opposite things. For lawmakers, security means eliminating uncertainty. For cryptographers, it means establishing guarantees within uncertainty. The two cannot coexist. When power chooses the former, then cryptography contradicts itself.

3 Freedom and fear

The philosophical question posed is simple: *what do we become when we trade freedom for protection?* As Hannah Arendt observed in her analysis of the politics of fear [2, 3], fear organizes obedience. Technological fear does so invisibly, by disguising obedience as optimization.

Isaiah Berlin distinguished between negative and positive liberty, freedom *from* interference versus freedom *to* be protected [4]. Langdon Winner argued that *artifacts have politics* [14], embedding decisions about authority into design itself. ChatControl illustrates how these two perspectives converge as a system that claims to protect users by technically enforcing their safety in fact constrains them through architecture. This is what we call *technological obedience*, a state in which compliance is produced by design rather than demanded by force.

True security is not the absence of danger but the presence of trust. The more we automate suspicion, the less trust remains for the institutions that claim to protect us. In this sense, ChatControl is not only unconstitutional in a legal sense but self-defeating in a scientific one as it replaces an epistemology of verification with an epistemology of suspicion.

Science practiced under fear mutates into bureaucracy. Its ethics shrink from "what is right?" to "what is permitted?". This is how undone science begins. Not through censorship but through exhaustion. When researchers internalize the limits of what can be asked.

4 The moral responsibility of technical work

The lesson is not new. Abelson et al. demonstrate that CSS introduces systemic insecurity and transforms personal devices into surveillance nodes [1]. Rogaway argues that cryptography must account for the human welfare it shapes, or risk serving the very powers it once constrained [11]. Rosenbloom connects these insights to collective power, reminding us that "security" is lived unevenly across social groups [12].

Yet these remain minority positions. Our whole scientific ecosystem: venues, review culture, funding calls, treats ethics as context, not content. We produce definitions without declarations, proofs without positions. Thousands of pages on secure messaging say little about what security is *for*.

To reclaim moral agency, we must restore a sense of vocation to science. That means refusing tasks that contradict our discipline's founding promise which is to protect communication from coercion, whatever its source. It also means building professional habits that make ethics unavoidable: adversary-justification sections, social-impact appendices, ethical peer review. Each security theorem, helps draw the boundary of user agency, what the system permits, resists, or logs.

Seen through the lens of undone science, moral responsibility in technical work begins not after discovery but before it. It begins with choosing which questions to ask, which uncertainties to tolerate, and which risks to normalize. Ethical practice thus includes the deliberate refusal to let ignorance harden into infrastructure.

5 The undone science of liberty

Undone science here is not missing data or misrepresenting populations. It's about moral illiteracy institutionalized as neutrality. Our field can prove lemmas but cannot yet articulate the value it protects. This vacuum allows governments to co-opt our language and be able to call surveillance "safety" and backdoors "exceptional access". We cannot fix this with new cryptographic primitives. The solution is to cultivate moral imagination inside our offices (or wherever it is that we work from).

By extending Hess' concept of undone science to the domain of regulatory epistemology, this argument connects cryptography's moral crisis to broader debates in *undone computing*: how neglected empirical and ethical inquiry in technical fields reproduces structural blind spots in governance. Policy can't assume that algorithmic detection is reliable without establishing its limits.

We don't rise to the challenge by inventing better inspection, we do so by recovering the courage to say *no*. To decline projects that transform fear into infrastructure. If this sounds like activism, well it's not. This is scientific hygiene. A discipline that builds the foundations of trust must know when it is being asked to engineer its collapse.

6 Conclusion

ChatControl is a European proposal, but the dilemma it exposes is universal. How much freedom are we willing to surrender to feel safe? The answer can't come from cryptography alone, but cryptography witnesses it daily. In a world where the language of security is used to erode liberty, the moral task of science is to defend the very uncertainty that makes freedom possible. Choosing trust over fear can't be seen as some nebulous philosophy that we ponder about but it is maintenance that we do with the ongoing work of keeping the human meaning of security intact when institutions forget it.

For undone computing, this case reminds us that epistemic neglect is never neutral: the absence of inquiry is itself a moral decision, and restoring the priority of knowledge over fear is the first condition for aligning technological progress with human flourishing.

References

[1] Harold Abelson, Ross Anderson, Steven M Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G Neumann, Ronald L Rivest, Jeffrey I Schiller, Bruce Schneier, Vanessa Teague, and Carmela Troncoso. Bugs in our pockets: the risks of client-side scanning. *Journal of Cybersecurity*, 10(1), January 2024. URL: http://dx.doi.org/10.1093/cybsec/tyad020, doi:10.1093/cybsec/tyad020.

[2] Hannah Arendt. *The Origins of Totalitarianism.* Harcourt, Brace & Company, 1951.

[3] Hannah Arendt. *On Violence.* Harcourt, Brace & World, 1970.

[4] Isaiah Berlin. *Four Essays on Liberty.* Oxford University Press, 1969.

[5] Patrick Breyer. Danger to democracy: 500 scientists urge eu governments to reject chat control, 2025. URL: https://www.patrick-breyer.de/en/danger-to-democracy-500-top-scientists-urge-eu-governments-to-reject-technically-infeasible-chat-control/.

[6] Euronews. Fact check: Is the eu about to start scanning your text messages? Euronews, 11 Sept, 2025. URL: https://www.euronews.com/my-europe/2025/09/11/fact-check-is-the-eu-about-to-start-scanning-your-text-messages.

[7] European Commission. Proposal for a regulation of the european parliament and of the council laying down rules to prevent and combat child sexual abuse. EUR-Lex COM(2022) 209 final, 2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0209.

[8] David J. Hess. Undone science: Social movements, mobilized publics, and industrial transitions. In *Routledge Handbook of Science, Technology, and Society*, pages 141–157. Routledge, 2016.

[9] Sheila Jasanoff. *States of Knowledge: The Co-production of Science and Social Order*. Routledge, 2004.

[10] Open letter on the position of scientists and researchers on the EU's proposed child sexual abuse regulation. URL: https://csa-scientist-open-letter.org/Sep2025.

[11] Phillip Rogaway. The moral character of cryptographic work. Cryptology ePrint Archive, 2015. URL: https://eprint.iacr.org/2015/1162.

[12] Leah Namisa Rosenbloom. Cryptography and collective power. Cryptology ePrint Archive, 2024. URL: https://eprint.iacr.org/2024/1602.

[13] TechRadar. Chat control: Germany, belgium, italy, and sweden shift their positions ahead of the oct 14 meeting. TechRadar, Sept 2025, 2025. URL: https://www.techradar.com/computing/cyber-security/chat-control-germany-belgium-italy-and-sweden-shift-their-positions-ahead-of-the-october-14-meeting.

[14] Langdon Winner. Do artifacts have politics? *Daedalus*, 109(1):121–136, 1980.