CENTER FOR
CYBERSECURITY
POLICY AND LAW

WHITEPAPER

BEYOND BUZZWORDS: HOW PEOPLE ACTUALLY WEIGH PRIVACY, SECURITY, AND SAFETY UNDER SCANNING AND ACCESS MANDATES

Heather West and Frances Schroeder
Center for Cybersecurity Policy & Law

Introduction/Executive Summary

New research across the Nordic countries shows that public support for content scanning and government access to encrypted data is conditional. While respondents express support for these measures in the abstract, that support declines sharply when real-world constraints - such as the tradeoffs between content scanning and cybersecurity are introduced. When forced to choose, the majority of respondents prioritize protecting their privacy and securing their devices over efforts to prevent the spread of harmful content. The findings, explored in this paper, suggest three guiding principles for policymakers:

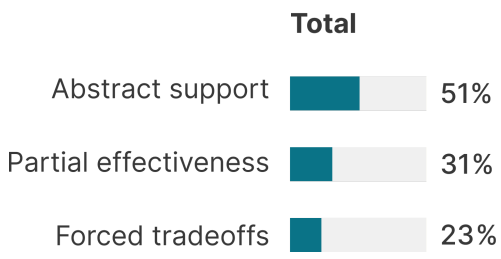
- Baseline security, data privacy, and strong encryption should be considered as foundational digital safety protections, not features to be traded away.
- Systemic mandates, such as broad-based content scanning proposals, that would alter encryption architecture for all users should be replaced with narrowly-tailored, case-specific measures tied to the identified harm.
- Such systemic mandates to redesign secure, end-to-end encrypted systems require independent evidence of effectiveness, clear necessity, and governance structures capable of sustaining public trust

Regulatory proposals intended to address the spread of illegal or harmful material online often present content-scanning and decryption mandates as straight-forward ways to address the spread of illegal or harmful material online or to support national security goals. These simplistic presentations neglect to note that content scanning mandates implicate foundational security architectures that are critical for the protection of public safety, devices, and digital services.

The Center for Cybersecurity Policy & Law commissioned original research across Nordic countries – specifically Sweden, Denmark, Finland, and Norway – to understand how people think about the complex privacy, security, and safety considerations that underlie these efforts. The results reveal a more nuanced set of public preferences than headline polling would suggest.

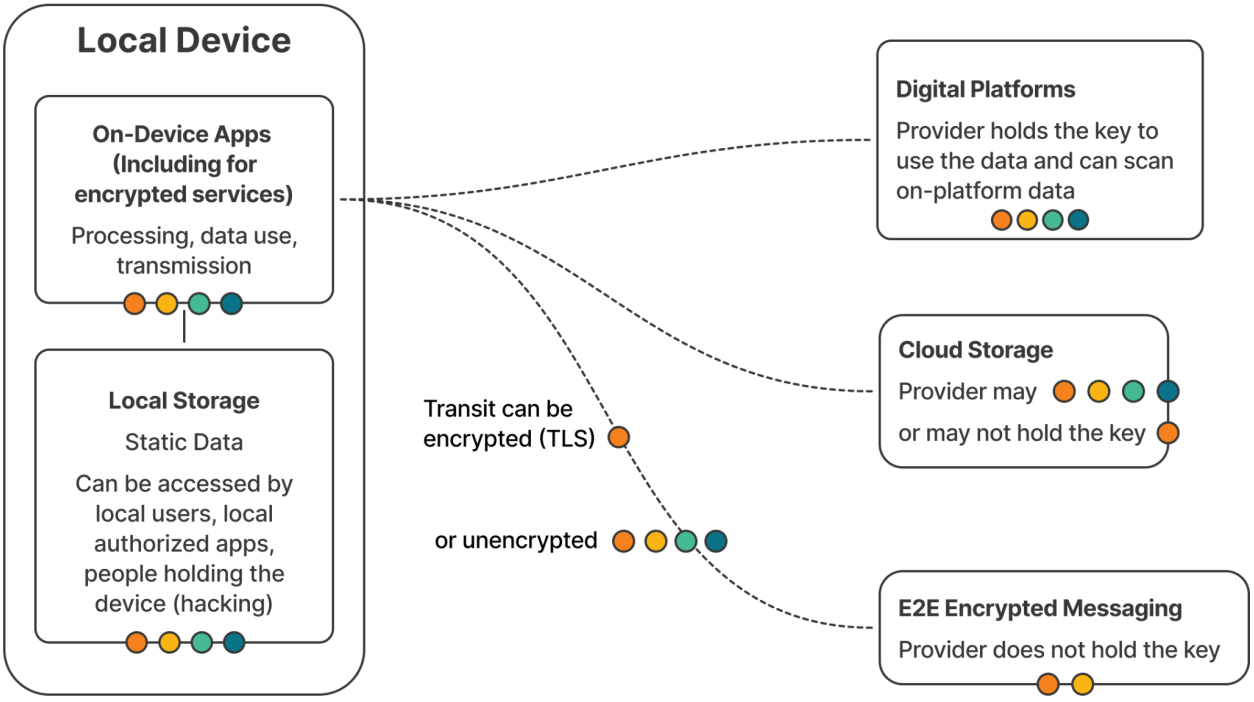
Respondents express support for scanning and government access to encrypted data in the abstract, but that support narrows sharply once operational limits, imperfect effectiveness, and cybersecurity tradeoffs are made explicit. When told that scanning would be only partially effective, support for content-scanning mandates fell significantly. And when asked to choose between competing priorities, majorities preferred protecting their privacy and securing their devices over measures designed to stop the spread of malicious or dangerous content.

Moreover, while many respondents endorse the claimed security and safety goals underlying scanning and access proposals, respondents diverged significantly on which institution should manage such initiatives – suggesting that no single institution commands the trust to do so. This presents a governance challenge that cannot be resolved by technical mandates.



Content Scanning and Exceptional Access

Scanning Method	Privacy Impact	Effectiveness	Security Impact
Metadata analysis	Lower	Lower	None
Hash matching	Lower	Limited	Minimal
Classifier-based	Higher	Broader	Moderate
Decrypting content	Higher	Broad	High (E2EE impact)



Content scanning refers to a spectrum of technical methods platform providers can use to screen content on their platforms to detect specific types of material. Scanning can take place server-side or client-side, and it can be used to analyze metadata or the content itself. Each content-scanning approach involves trade-offs between privacy and effectiveness.

Unfortunately, there is no perfect world in which scanning operates as a simple solution. Scanning detection systems have limitations and backdoors may present a new cybersecurity risk. Hash-matching can identify known material but not new or even modified content. Classifier-based systems can attempt to identify unknown material, but they inevitably generate both false positives and false negatives. Ultimately, malicious actors can adapt their tactics in response to detection methods. As a result, scanning may reduce certain categories of risk, but it cannot be perfectly effective especially against new and unknown content.

Exceptional access refers to a variety of technological and design features that enable access to encrypted communications. End-to-end encryption is designed so that *only* communicating users can read message content; even the technology provider does not have access to the content. Providing "exceptional access" for a third party, such as a law enforcement entity, requires altering that architecture, either by creating a backdoor into secure encryption, or by downgrading to less secure encryption. Any such mechanism changes the security model by introducing additional access to new players and new key management requirements. Importantly, such a pathway exists for authorized actors, it can also be targeted by unauthorized ones. Malicious actors, who routinely probe high-value targets for access points, would have strong incentives to discover and exploit the same pathway.

Both content scanning and exceptional access require companies that have built end-to-end encrypted systems to change the underlying security architecture of these services and often preclude the implementation of additional security protections. These changes potentially introduce new security vulnerabilities or limit security protections that might otherwise apply.

The Survey

The Center partnered with a research agency to survey 8,002 respondents across Sweden, Denmark, Finland, and Norway about how they think about online privacy, security, and safety, and to understand how they prioritize each. The survey was conducted through online interviews between December 2-16, 2025, using nationally representative quotas for age, gender, and region. The research also explored respondents' familiarity with topics such as scanning and encryption and how people protect themselves online. Below are our major findings.

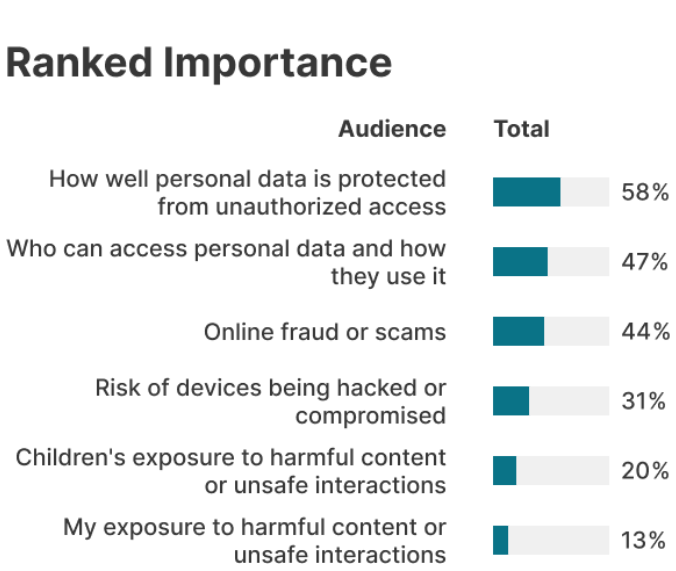
People Distinguish Privacy, Security, and Safety – But Link Them Through Hacking and Unauthorized Access

We surveyed people on how they define the concepts of online safety, security, and privacy. The responses demonstrate that Nordic people do not treat privacy, security, and safety as interchangeable. Instead, people distinguish them, but there is some overlap. People define them through a shared lens centered on unauthorized access, hacking, and misuse.

- **Online privacy** was consistently described as the ability to keep their personal information safe, confidential and under their own control. People emphasized a desire to decide who can see what, stay anonymous, and avoid hacking, scams, tracking, misuse of data or unwanted exposure.
- **Online security** is seen as protection against adversarial harms such as hacking, fraud, and malware. People associate this with tools like VPNs, antivirus software, firewalls, and strong passwords to ensure their data stays private, safe, and shielded from criminals.

- **Online safety** was described consistently as the ability to use the internet without fear of scams, hacking, data theft, or harmful content. Responses reflected that people have a strong desire for trust, security, and peace of mind when engaging online.

All of these concepts were seen as important, though in varying ways, as we explore below.



Privacy and Security Outrank Harmful-Content Concerns

The results show that people prioritize core privacy and security factors above all other online well-being factors in this survey, including exposure to harmful content, unsafe interactions, and children's online risks. Across the Nordics, individuals consistently placed the highest importance on protecting their personal data from unauthorized access, controlling who can access their information, avoiding fraud or scams, and preventing devices from being hacked. That is, they cared more about protection from unauthorized access, fraud, and hacking than about both their own exposure to harmful content and children's exposure to harmful or unsafe interactions.

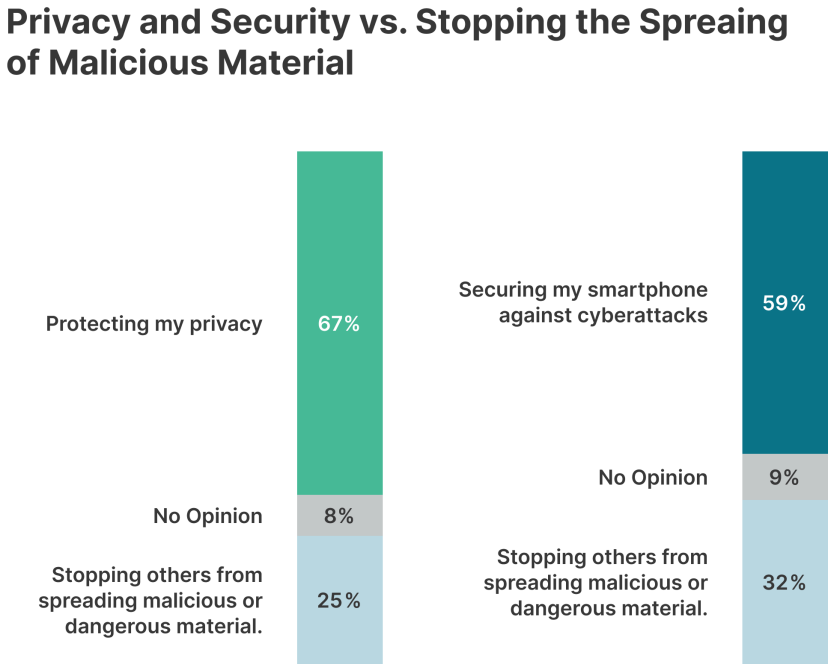
While concerns about harmful content are widely deemed as important across the Nordic region, particularly among those with kids, personal security and privacy factors are prioritized as more important than concerns related to harmful content, including both personal exposure and children's online safety risks.

When asked to rank the importance of various online well-being factors in day-to-day use, respondents consistently prioritized privacy and security items ahead of content safety considerations when ranking a defined set of online well-being factors, including exposure to harmful content, unsafe interactions, fraud, and device compromise. In order of importance, respondents ranked protecting personal data from unauthorized access, online frauds or scams, who can access their personal data and how it is used, and risk of devices being hacked or compromised ahead of both children's exposure to harmful content or unsafe interactions and their own exposure to harmful content or unsafe interactions.

Overall, all of these online wellbeing factors are seen as important, but concretely asking respondents to prioritize what is most important had clear impacts on the results. When asked to rank what they care about most, harmful-content exposure (especially their own personal exposure)

is least likely to be placed at the top among the factors tested (unauthorized access, fraud, hacking, data control, and content-related harms), while unauthorized access, scams, and hacking dominate priority rankings. This does not suggest respondents disregard harmful content. Rather, when placed alongside concrete risks such as fraud or hacking, those risks tend to take precedence.

When Forced to Choose, Majorities Prefer Privacy and Device Security

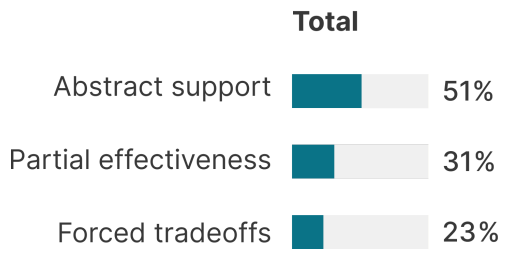


We presented respondents with specific choices: protecting their privacy or stopping others from spreading malicious or dangerous material, and securing their smartphone against cyberattacks or stopping others from spreading malicious or dangerous material. These tradeoffs gave respondents a chance to consider whether they would prioritize secure digital architectures or access for content scanning. When respondents were presented with these explicit tradeoffs:

- 67% chose protecting their privacy over stopping others from spreading malicious or dangerous material.
- 59% chose securing their smartphone against cyberattacks over stopping malicious material.

These results demonstrate that when privacy and security and content moderation are placed in tension, privacy and device security win clear majorities over content-control objectives in direct tradeoff scenarios.

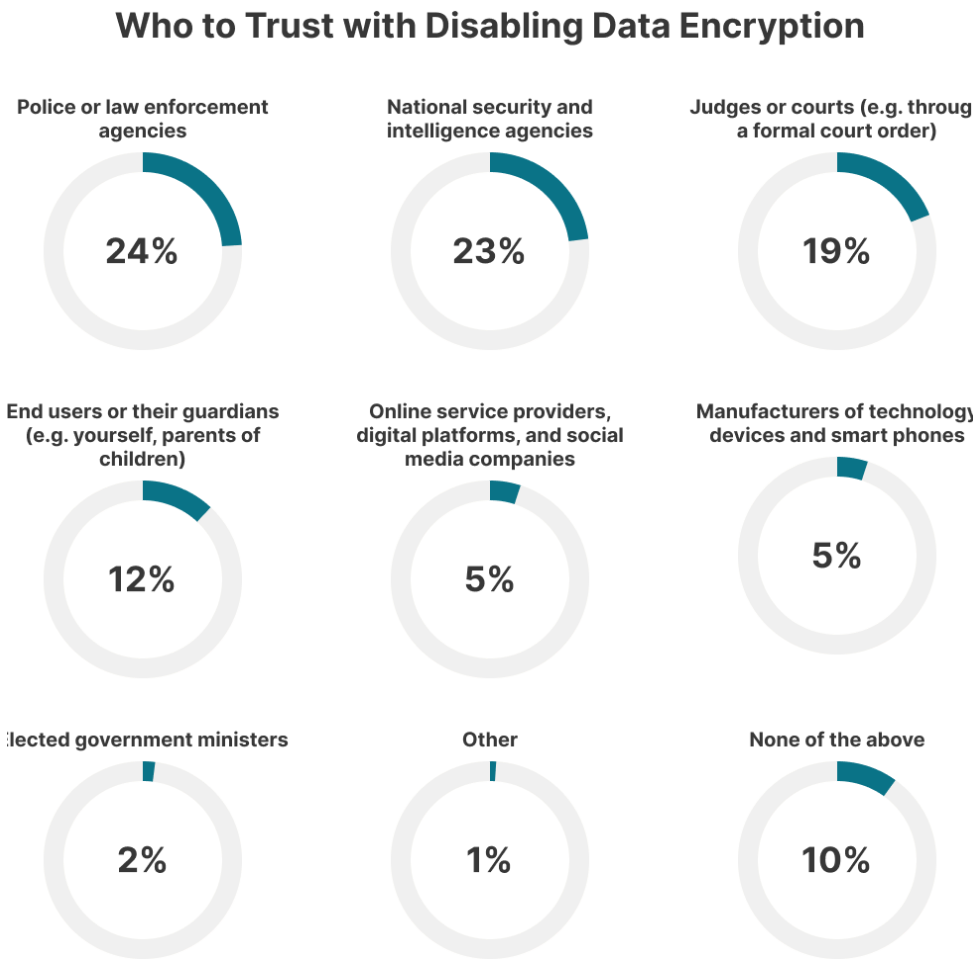
Support for Mandatory Scanning Drops Under Partial Effectiveness



We then asked respondents about their support for mandatory scanning. We found that support for mandatory scanning on online services (e.g. Facebook, iMessage, WhatsApp) is high in the abstract (51%). Support for mandatory scanning drops slightly for digital storage platforms (e.g. Google Drive, iCloud) and their own tech devices.

However, only 31% still support mandatory scanning if it is not *entirely* effective, indicating that people support the goals behind these proposals, but may not support the practice. This demonstrates that abstract support is premised on assumptions of high effectiveness. Once scanning is framed realistically, as an imperfect tool, support becomes a minority position.

Exceptional Access Lacks a Broadly Trusted Authorizer



The majority (72%) of respondents indicated they have some basic knowledge of data encryption, with greater familiarity among younger generations and the Finnish. We asked which kinds of data

should be encrypted, and most people in the Nordics believe it is important that all types of data are encrypted, with financial information being the most widely recognized as important – but all types of data had over 87% other than online browsing history, which was 76%.

Support for law enforcement access to encrypted data is high in the Nordics, with over half supporting even if disabling encryption could introduce vulnerabilities that could be exploited by hackers or foreign governments. However, when asked what institution should be responsible for this access, it was clear that there was not a broadly accepted entity to play that role.

There is no single authority that people trust to have access to decrypted data, as no institution emerges as a majority-trusted actor to authorize disabling encryption. This highlights that while people support mandatory access in theory, they cannot identify any entity that they trust to wield that power. This fragmented trust base creates a governance challenge for exceptional-access frameworks.

Principles for Policymakers

This research points toward three principles that should guide policymaking in this space. These principles do not reject the importance of combating serious online harms. Instead, they reflect how respondents themselves weigh privacy, security, and safety when confronted with real tradeoffs.

Baseline Security and Privacy First

Across the Nordic countries surveyed, respondents consistently ranked protection against unauthorized access, fraud, scams, and device compromise above both personal exposure to harmful content and children's online safety risks. When asked to prioritize what matters most in day-to-day online life, personal data protection and protection against hacking outranked all other concerns included in the survey's ranking exercise, particularly content-related harms. Clear majorities selected protecting their privacy and securing their devices over stopping the spread of malicious material.

These results suggest that strong encryption and device security are viewed as baseline protections rather than optional features to be traded away. Policymakers should begin from a presumption in favor of preserving robust end-to-end encryption and secure system architectures. Any proposal that would systematically weaken encryption or mandate generalized scanning of private communications should proceed only where the necessity is clearly demonstrated, the scope is narrowly tailored, and the security tradeoffs are proportional to measurable gains. Otherwise, such mandates risk undermining the very forms of safety – freedom from hacking, fraud, and unauthorized access – that citizens prioritize most.

Legislatures should require a formal privacy and cybersecurity impact assessment for any proposal involving content scanning or exceptional access. This assessment should evaluate risks across personal, enterprise, and government systems, including potential exploitation pathways introduced by new access mechanisms.

Targeted Tools Over Systemic Mandates

Support for scanning and exceptional access is weaker relative to abstract support levels when respondents are presented with operational constraints and tradeoffs. Only one in three respondents would continue to support mandatory scanning if it were only partially effective. At the same time, no single institution commands even a quarter of respondents' trust to authorize disabling encryption.

This conditional support and fragmented trust argue against broad, architecture-level mandates. Instead of universal backdoors or blanket scanning obligations, **policymakers should prioritize targeted, case-specific investigative tools that operate under judicial authorization and clear procedural safeguards.** Targeted tools should be defined as those that operate on specific accounts, devices, or investigations under judicial authorization, without introducing persistent access mechanisms into the broader system architecture.

Case-specific endpoint access pursuant to lawful process, strengthened cross-border cooperation, and focused disruption of criminal networks offer avenues for enforcement that do not require altering encryption architecture for all users. Unlike systemic backdoors, these tools operate in defined cases, under judicial authorization, without introducing persistent vulnerabilities into the broader ecosystem.

Evidence Before Expansion

Public support for scanning appears to require an implicit assumption of high effectiveness. Unfortunately, detection systems are inherently imperfect, generating both false positives and false negatives, and adversaries adapt over time. Once respondents were told that scanning would be only partially effective, support fell sharply.

Policymakers should not legislate based on idealized performance. Before imposing mandates that require architectural redesign of secure systems, legislatures should require independent technical validation of effectiveness, transparent public reporting of false positive and false negative rates, and periodic legislative reassessment of both efficacy and security impacts. Exceptional-access frameworks, in particular, should be conditioned on demonstrable necessity, narrowly defined scope, and institutional oversight mechanisms capable of sustaining public trust. Where evidence does not show substantial, measurable gains that outweigh systemic security risks, mandates should not proceed.

These principles reflect a coherent reading of the data: citizens value safety, but they define it largely through strong privacy and security protections. Effective policy in this domain must protect those foundations while pursuing harm reduction through proportionate, accountable, and evidence-driven means. **Legislation should require publicly reported performance benchmarks, including false positive and false negative rates under realistic conditions, as well as periodic reassessment tied to measurable outcomes.**

Conclusion

Our research found that Nordic respondents care deeply about safety, but they define safety through a framework that includes protection from hacking, scams, and unauthorized access. When forced to prioritize, they place privacy and device security above stopping malicious material, and when scanning is presented as only partially effective, support drops to a minority.

For respondents, safety is not primarily defined as preventing exposure to harmful speech or material. Instead, it is seen as protection against adversarial misuse. Policies that degrade encryption are likely to undermine the safety that citizens prioritize.

Legislatures should not evaluate scanning or exceptional access proposals under best-case assumptions. Public support appears to be based on near-perfect efficacy, but detection systems generate false positives and false negatives, and adversaries adapt. Policymakers should require empirical performance benchmarks and independent validation before imposing systemic obligations. These frameworks will only be accepted with clear, trusted governance in place.

These findings suggest that regulation should be risk-calibrated and evidence-driven, and should avoid systemic weakening of secure communications. Public opinion is not aligned with a workable model of universal scanning or exceptional access. Instead, the evidence suggests that policymakers should preserve strong baseline security while pursuing narrowly tailored, accountable, and empirically validated interventions against serious harms.