PRIVACY

BLOCKCHAIN FOR EUROPE

Context

Public blockchain networks are transparent by design. All transactions are recorded on the shared public ledger, allowing anyone to scan a public blockchain address and view the entire transaction history, including holdings and transfers for each token, from the moment the address was created. This level of transparency does not exist in traditional financial services where information is shielded. For example, no one can simply scan an IBAN or account number to view the full history of transactions and payments of that account - such data is only accessible to authorized parties, financial institutions or governments. The lack of transparency in traditional financial services is a critical feature because it protects European privacy principles, complies with legal obligations under data protection frameworks such as GDPR, and reduces the risk associated with the exposure of financial information. One's financial data is just as much a financial asset as the instruments one owns.

To address the lack of privacy on-chain, developers are working on privacy-enhancing solutions and tools (PETs). These tools align with the EU legal framework that enshrines privacy as a fundamental right. Users of blockchain wallets have legitimate reasons to desire privacy on a blockchain. For example, a pensioner may wish to protect their accounts from prying eyes, or an activist in an authoritarian regime may need to shield their financial activity including donations from surveillance to avoid persecution. There is also no reason that a person using their wallet to pay a merchant or receiving digital art from a friend should suddenly have their entire transaction history exposed to that merchant or that friend.

Why does it matter?

Privacy is a fundamental principle and legitimate use-case

The European Union has a long and distinguished history of protecting the privacy of its citizens and recognises privacy as a fundamental freedom. It has an extensive and well-developed legal framework, built on the foundations of the EU Charter of Fundamental Rights, which includes the EU General Data Protection Regulation (GDPR), the Data Protection Law Enforcement Directive, and institutions such as the European Data Protection Board or the European Data Protection Supervisor to oversee the application of data protection rules.

As seen from these examples, privacy protections extend across both public and private sectors and demonstrate the EU's commitment to ensuring that privacy remains a core principle of all interactions. As such, PETs are a natural extension of the EU's commitment and embody principles of privacy and data protection. PETs offer indispensable benefits and enable individuals to shield their financial activities from unnecessary exposure and to protect their own data.

Developers should not be held liable for misuses of their open-source software

The role of open-source software developers in advancing technological innovation in the field of privacy cannot be overstated. However, some mistakenly argue that developers should bear responsibility for how their tools are used, even when those tools are neutral and autonomous by design. Such liability would not only hinder technological progress in PETs but could have a broader chilling effect on innovation across the tech sector.

In an increasingly globalized world, highly skilled workers may opt to relocate to jurisdictions that support and incentivize innovation, potentially diminishing the EU's competitiveness in emerging technologies. In fact, developers should be encouraged and empowered to further innovation in privacy preserving technologies and to ensure that PET tools are widely available to users. Placing liability on developers for misuse of their code would mark a dangerous and unprecedented departure from existing and established legal norms. This could also undermine economic opportunities for Europe, with restrictive policies potentially pushing developers and businesses toward markets like the US or China, further entrenching Europe's dependency on foreign technology leaders. From a security and defence perspective, driving innovation elsewhere risks creating technological dependencies on companies outside the EU that may not align with European values or standards. This could increase risks to EU citizens, including exposure to data misuse by foreign adversaries or vulnerability to interference.

We must thus resist any attempts to hold developers of neutral privacy tools liable for how their code is used and we must reject any notion that the privacy tools themselves are being vilified for their dual use nature, as though the privacy itself is inherently suspicious. We must also resist any attempts to broadly outlaw PETs under the guise of preventing misuse. Historically, software developers have not been held accountable for how their software is used and there is no rationale to impose such burdens on open-source creators now. Such liability would result in developers being forced to prioritise avoiding liability over pursuing groundbreaking solutions, therefore slowing technological progress, weakening privacy protections in digital space and undermining the fundamental principles of open collaboration.

Position

Principles to underpin all EU policy and regulatory initiatives related to privacy and technology:

1. **PETs are essential for safeguarding online privacy.** They are indispensable for protecting an individual's autonomy, self sovereignty and human dignity. PETs tools serve as a broader public good, they are not just beneficial but essential for the healthy functioning of the internet, including decentralized systems, and ultimately for a free, open and equitable society.

2. **Developers should not be penalized for advancing technology and for creating neutral privacy tools.** Holding developers liable for potential misuse of the tools they create risks stifling innovation, depriving society of essential technological advancements and threatening the principles of privacy and freedom at the core of the digital age.

In the digital-first world, privacy is not a luxury or convenience but a fundamental human right, a necessity. Privacy is also not an optional privilege that can be granted or revoked based on subjective criteria but a fundamental value that has to be embedded by default into digital frameworks and that should underpin any digital architecture and infrastructure. PETs play a critical role in fostering secure, decentralized and neutral internet. By recognizing PETs as essential and safeguarding developers from undue liability, the EU can reaffirm its leadership in privacy and data protection as cornerstones of digital sovereignty while paving the way for a more secure and equitable digital future, open diverse and pluralistic societies free from unchecked mass surveillance and systemic intrusions into individuals' private lives.