Encryption: A Powerful Way to Achieve Citizen Privacy with High Economic Gains

December 2021

Digitized systems represent incredible opportunities for efficiency and growth, but they also create vulnerabilities. The exponential growth of the internet is driving an increase in the risk factors associated with daily threats to sensitive information, the financial system and vulnerable devices/infrastructure. Encryption, the method of transforming data by a cryptographic algorithm to produce ciphertext, i.e. to hide the information content of the data, has been a longstanding way for sensitive information to be protected. Undoubtedly, encryption is at the core for the functionality of critical sectors such as finance, health and, information and communications. A privacy-enhancing tool for citizens, encryption is an enabler of human rights reflecting societal value to state and citizenry alike as it helps shield citizens and companies from fraud, hacking, and corporate espionage by safeguarding everything from financial transactions to everyday consumer devices.

Incidents such as the Greek Watergate scandal (Spinellis and Prevelakis, 2007) and the most recent data breach involving Air India, Domino's and Big Basket which compromised the emails and passwords of hundreds of Union government ministers, exposing them to cyber threats. These all serve as potent reminders of the importance of properly securing our ever-expanding digital world. Strong encryption is our best tool in the 21st century for ensuring that the damage and costs of cyberattacks, data breaches, and other types of exposure remain minimized.

Back in 2018, Australia passed an aggressive encryption bill that gives the government's security and intelligence agencies the legal authority to compel tech companies to break their encryption. The tech companies are required to provide law enforcement and security agencies with access to encrypted communications. However, the bill has significantly degraded the global reputation of the Australian tech sector, as there is a notion that the Act will degrade industry's ability to secure customer data and place their employees at individual peril. So, nations across the globe need to take a more positive approach to encryption.

Despite national security benefits, encryption has been viewed negatively by law enforcement as a barrier to investigation, and a threat to national security and public order. The debate, initially a clash between privacy and national security, has now shifted to security versus security debate. Aapti, a public research institute that works on the intersection of technology and society, examines the ways in which people interact and negotiate with technology both offline and online. In Nov 2021, Aapti published a report, "Unpacking Social and Economic Gains from Encryption". As per the report, encryption must not only be viewed through the narrow lens of national security, but from a broader perspective capturing its economic and societal value. For the nation, encryption boosts national economy, national security, and is an enabler of human rights. For the citizen, encryption is a tool protecting the right to privacy and free speech, and allows availing of a plethora of services and products enhancing consumer satisfaction. For the firm, encryption facilitates user trust and accelerates product innovation.

The core value of encryption technologies is user trust, foundational to the broader goals of digitalization. The economic, monetary, reputational, privacy and security incentives flow from user trust. Research indicates that users of E2EE platforms are likely to stop sharing different kinds of information such as personal photographs and videos, video and audio calls, identification documents, religious and political views in the absence of encryption (CUTS n.d.). As many as 75% of respondents feared an increase in the likelihood of unintended recipients accessing their chats (CUTS n.d.).

Aapti's quantitative analysis utilizes the Global Cybersecurity Index (GCI), a comprehensive measure of five pillars of general cyber security adoption, and the Privacy Index (internally coded) assessing individual and societal legal frameworks around privacy at a country level- both strongly positively correlated with GDP per capita, significant at the 95% level. These metrics capture the complex nature of E2EE enabling apt conceptualization of encryption as a techno-societal solution. Quantitative analysis indicates that doubling a nation's score on the GCI is associated with a ~$2700 increase in GDP/capita. The coding on legal frameworks that protect end-to-end encryption (E2EE) suggests a positive relationship between such legislation and participation in the digital economy and GDP per capita.

Encryption is a techno-societal solution. In addition to being a technological solution to cyber threats, it possesses societal value by accelerating economic growth and social development. It fulfils societal goals of instilling user trust – a key to economic growth. A strong encryption policy is bolstered by a number of resilience frameworks – technical, legal, societal and institutional. Resilience is critical as the pace of technology will continue to try and decrypt data. Technical solutions around encryption will only have real value if there is better institutional and societal capacity, undergirded by strong legal frameworks. Firms develop technical solutions that propel creation of data security measures and adopt data and privacy protecting practices that strengthen their institutional capabilities to combat cyberthreats. Societal resilience posits citizens as the focal point of data protection, creating enabling environments that shield citizens from cyberthreats. Legal resilience allows the institutionalization of data protection principals guiding privacy frameworks in the state.

As the risks and damages of security breaches and data exposure increase, so too do the consequences of failing to implement and support strong encryption. A collaborative approach by all key stakeholders - firms, law enforcement, law and policy makers, and the government machinery, is needed for putting in place a robust encryption policy.