Undergraduate Thesis Prospectus

The Struggle over End-to-End Encryption in the United States

(sociotechnical research project)

by

Nurbol Lampert

November 8, 2024

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Nurbol Lampert

STS advisor: Peter Norton, Department of Engineering and Society

General Research Problem

How can encryption technologies balance the need for user privacy with the demands of national security and law enforcement?

Encryption secures digital communications and protects sensitive data. As society relies more on digital platforms, robust encryption safeguards against cyber threats and unauthorized access. However, encryption also challenges law enforcement and national security agencies by hindering access to information crucial for preventing and investigating crimes. The "going dark" problem refers to the loss of access to communications due to encryption, which authorities argue impedes criminal investigations (U.S. Department of Justice, 2019). Balancing user privacy with law enforcement needs is complex, with significant implications for technology, governance, and individual rights.

The Struggle over End-to-End Encryption in the United States

In the U.S., how have privacy advocates, regulators, and tech companies competed to influence the priority of user privacy, digital security, and law enforcement in encryption?

End-to-end encryption (E2EE) stands at the center of U.S. debates over privacy, security, and law enforcement access. While encryption protects users' privacy and secures communications against cyber threats, it also complicates efforts by law enforcement agencies to access data critical for investigating crimes and ensuring national security. This conflict arises from differing perspectives on whether encryption should be absolute or if exceptions should be

made for government access. The debate has significant implications for individual rights, cybersecurity, and the balance of power between citizens and the state.

Privacy advocates argue that any weakening of encryption compromises the security of all users. The Electronic Frontier Foundation (EFF) warns that "any vulnerability in encryption is a vulnerability for all users" (EFF, 2015). They maintain that strong encryption is essential for protecting personal data and safeguarding civil liberties. Similarly, the American Civil Liberties Union (ACLU) emphasizes that "weakening encryption for one purpose weakens it for all purposes" (ACLU, 2023). These groups contend that introducing backdoors or exceptional access mechanisms would create vulnerabilities exploitable by malicious actors, leading to mass surveillance and violating citizens' rights to privacy. Tech companies like Apple and WhatsApp are caught between these opposing pressures. Committed to user privacy and security, they resist government demands for backdoors. In response to a government request to unlock an iPhone involved in a criminal investigation, Apple asserted, "We fear that this demand would undermine the very freedoms and liberty our government is meant to protect" (Apple Inc., 2016). Apple maintains that creating backdoors would compromise the security of all users and set a dangerous precedent. Will Cathcart, head of WhatsApp, declared, "We will always oppose government attempts to build backdoors because they would weaken the security of everyone who uses WhatsApp" (Cathcart, 2021). These companies argue that strong encryption is necessary to protect users from cyber threats and maintain trust in their products. Civil liberties groups like the Center for Democracy & Technology (CDT) support strong encryption as essential for free expression and privacy. The CDT warns that "mandating backdoors or exceptional access would undermine security and privacy for everyone" (CDT, 2017). They

engage in policy advocacy to influence legislation and public opinion, emphasizing that any weakening of encryption could be exploited by authoritarian regimes and threaten global human rights.

Government agencies such as the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) advocate for lawful access to encrypted data. Attorney General William Barr expressed concern that encryption is enabling criminals to "hide their activities from law enforcement" (DOJ, 2019). The DOJ argues that encryption impedes criminal investigations and poses a threat to public safety and national security. FBI Director Christopher Wray stated, "We face an enormous and increasing number of cases that rely heavily, if not exclusively, on electronic evidence" (FBI, 2020). These agencies seek mechanisms that would allow access to encrypted communications under legal authority, asserting that without such access, they cannot effectively protect the public. Law enforcement organizations, including the National Sheriffs' Association and the International Association of Chiefs of Police, support the government's position. In a joint statement, they asserted that "the inability to access encrypted communications poses a grave threat to public safety" (Law Enforcement Coalition, 2018). They argue that encryption hampers investigations into serious crimes such as terrorism, child exploitation, and drug trafficking. These organizations advocate for policies that would require tech companies to provide access to encrypted data under lawful authorization.

Cybersecurity experts and academics contribute to the debate by highlighting technical challenges and risks associated with introducing backdoors. In their influential paper "Keys Under Doormats," leading cryptographers argued that "providing access to communications data pursuant to law enforcement requests would pose unacceptable risks to cybersecurity" (Abelson

et al., 2015). They emphasize that any system providing exceptional access for law enforcement could also be exploited by hackers and foreign adversaries, undermining overall security. International developments influence the U.S. debate. Governments like the United Kingdom and Australia have enacted laws requiring technology companies to assist in accessing encrypted data (Australian Government, 2018). The Five Eyes intelligence alliance, which includes the United States, has collectively called for access to encrypted communications (Five Country Ministerial, 2018). These international pressures set precedents and impact domestic policy discussions.

This conflict reflects broader concerns about trust in technology, state power, and personal freedom. The encryption debate embodies tensions between security needs at individual and national levels. While encryption protects against cyber threats and preserves privacy, it complicates efforts to combat crime and terrorism. This tension raises questions about the appropriate balance between privacy rights and security needs. The concept of the "balance of power" between the state and individuals is relevant here (Nye, 2011). Encryption technologies shift power toward individuals by enabling private communication inaccessible to the state. This shift challenges traditional notions of state authority and surveillance capabilities. Government agencies argue that without access to encrypted data, they cannot fulfill their duty to protect the public, invoking social contract theory where citizens grant the state certain powers for protection.

However, privacy advocates contend that excessive surveillance infringes on individual rights and can lead to abuse of power. They argue that the government's demand for backdoors represents an overreach that threatens democratic freedoms. The "privacy paradox" complicates this debate, describing the discrepancy between individuals' stated privacy concerns and their

actual behavior (Barnes, 2006). While users demand strong encryption for privacy, they often share personal data freely on digital platforms, raising questions about the actual value users place on privacy versus convenience. Economic implications are significant. The tech industry argues that weakening encryption could harm the U.S. economy by undermining consumer trust and making American products less competitive globally (Business Software Alliance, 2015). Strong encryption is seen as essential for protecting intellectual property, fostering innovation, and maintaining a competitive edge in the global market.

High-profile cases have intensified the debate. The 2015 San Bernardino shooting brought the issue to the forefront when the FBI sought Apple's assistance to unlock the shooter's iPhone. Apple's refusal highlighted the conflict between law enforcement needs and corporate commitments to user privacy (Apple Inc., 2016). The case sparked public debate, with both sides leveraging media and legal avenues to advance their positions. Legislative proposals like the EARN IT Act aim to combat child exploitation by holding tech companies accountable if they fail to assist law enforcement (U.S. Congress, 2020). Critics argue that such legislation threatens encryption and could lead to censorship and privacy violations. The legal landscape remains unsettled, with ongoing court cases and legislative efforts shaping the future of encryption policy.

References

Abelson, Anderson, Bellovin, Benaloh, Blaze, Diffie, and Weitzner (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, 1(1), 69–79.

Abomhara, M., and Køien, G.M. (2015). Security and privacy in the Internet of Things: Current status and open issues. *Computer Communications*, 36(6), 45–52.

ACLU (2023, Oct. 20). American Civil Liberties Union. The Vital Role of End-to-End Encryption. www.aclu.org/news/privacy-technology/the-vital-role-of-end-to-end-encryption

Apple Inc. (2016, Feb. 16). Customer Letter: Your Security and Privacy Are Important. www.apple.com/customer-letter/

Australian Government (2018). *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*. www.legislation.gov.au/Details/C2018A00148

Barnes, S.B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9).

Business Software Alliance (2015). Encryption: Security in a High Tech World. https://www.bsa.org/files/reports/BSA_encryption_primer.pdf

Cathcart, W. (2021, Mar. 17). Why WhatsApp is pushing back on NSO Group hacking. WhatsApp Blog. https://www.business-humanrights.org/en/latest-news/commentary-why-whatsapp-is-pushing-back-on-nso-group-hacking/

CDT (2017). Center for Democracy & Technology. CDT's Comments on Law Enforcement Access to Data Stored Across Borders. https://commission.europa.eu/document/download/9fd2223e-a50e-45d9-a566-fc08967844da_en?filename=cdt_2017_en.pdf

EFF (2015, Dec. 31). Electronic Frontier Foundation. Encryption in the Balance: 2015 in Review. www.eff.org/deeplinks/2015/12/encryption-balance-2015-review

FBI (2020, Jan. 27). Federal Bureau of Investigation. Going Dark: Lawful Electronic Surveillance in the Face of New Technologies (testimony). www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies

Five Country Ministerial (2018). Statement of Principles on Access to Evidence and Encryption. https://www.homeaffairs.gov.au/nat-security/Pages/statement-of-principles-on-access-to-evidence-and-encryption.aspx

Green, M., and Smith, M. (2016). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, 2(1), 69–78.

Law Enforcement Coalition (2018). Joint Law Enforcement Statement on Encryption and Public Safety. https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

Nye, J.S. (2011). *The Future of Power*. PublicAffairs.

Rogers, E.M. (2003). *Diffusion of Innovations* (5th ed.). Free Press.

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.

Tajfel, H., and Turner, J.C. (1979). An integrative theory of intergroup conflict. In W.G. Austin and S. Worchel (Eds.), *The Social Psychology of Intergroup Relations* (pp. 33–47). Brooks/Cole.

U.S. Congress (2020). *Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020*, S. 3398, 116th Congress. www.congress.gov/bill/116th-congress/senate-bill/3398

DOJ (2019, Oct. 4). U.S. Department of Justice. Attorney General William P. Barr Delivers Remarks at the Lawful Access Summit (speech). www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-lawful-access-summit